



Dr.WEB®
Security Space

Benutzerhandbuch

Defend what you create

© Doctor Web, 2015. Alle Rechte vorbehalten.

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes darf ohne Quellenangabe reproduziert, auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanälen und Massenmedien verbreitet werden, ausgenommen der Nutzung für persönliche Zwecke.

WARENZEICHEN

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk und Dr.WEB Logos sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, oder Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS

Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfällen), die sich dadurch ergeben.

Dr.Web Security Space
Version 10.00.3
Benutzerhandbuch
04.08.2015

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Webseite: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website.

Doctor Web

Doctor Web ist ein russischer Anbieter hausgener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei der Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie ein global weit verbreitetes Nutzer-Netzwerk zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken allen Benutzern für ihre Unterstützung und Treue in Dr.Web Produkte!



Inhaltsverzeichnis

Kapitel 1. Einführung	6
Symbole und Hervorhebungen	6
Hauptfunktionen der App	6
Systemanforderungen	7
Kapitel 2. Lizenzierung	8
Testzeitraum aktivieren	9
Lizenz kaufen	9
Lizenz aktivieren	10
Lizenz verlängern	12
Kapitel 3. Installation und Deinstallation	13
App installieren	13
App deinstallieren und aktualisieren	14
Kapitel 4. Mit der Arbeit beginnen	16
App starten und beenden	16
Oberfläche	16
Widgets	18
Benachrichtigungen	18
Mein Dr.Web	20
Kapitel 5. Programmfunktionen und -einstellungen	21
Virenschutz	22
Permanenter Virenschutz	22
Überprüfung auf Anforderung des Benutzers	23
Neutralisierung der Bedrohungen	25
Bedrohungen bei Systemanwendungen entdecken	26
Sperr-Software bearbeiten	27
Anruf- und SMS-Filter	28
Filtermodus wählen	28
Blacklist	29
Filterprofil erstellen	30
Gesperrte Anrufe und Nachrichten einsehen	31
Aktualisierung	31
Quarantäne	32
Statistik	33
Dr.Web Diebstahlschutz	34
Ersteinstellung	35
Erweiterte Optionen einstellen	37
Freundesliste	38



SMS-Befehle	39
Dr.Web Diebstahlschutz-Sperre aufheben	40
Zugriff auf Internet-Inhalte einschränken	41
Dr.Web Firewall	42
Mobiles Internet einschränken	44
Anwendungsdatenverkehr behandeln	46
Aktuelle Aktivität der Netzwerkverbindungen	49
Ereignisse registrieren	50
Bei Beseitigung der Sicherheitslücken helfen	51
Kurz-URL-Dienst	54
Kapitel 6. Zentralschutz-Modus	55
In Zentralschutz-Modus wechseln	55
Anwendungsfiler	57
In eigenständigen Modus wechseln	57
Kapitel 7. Dr.Web für Android TV	58
Anhang	59
Anhang A. Technischer Support	59
Schlagwortregister	60



Kapitel 1. Einführung

Vielen Dank, dass Sie sich für **Dr.Web Security Space** (nachfolgend **Dr.Web** genannt) entschieden haben! Diese Antivirenlösung bietet einen zuverlässigen Schutz für mobile Geräte unter Android™ sowie Fernseher, Mediaplayer und Spielekonsolen unter Android TV™ vor diversen Arten von Schadsoftware, welche die Sicherheit mobiler Geräte bedrohen.

Im Programm wurden die meist fortgeschrittenen Konzepte und Technologien von **Doctor Web** eingesetzt, mit denen sich die Malware-Objekte, durch welche die Funktion und Informationssicherheit des Geräts gefährdet werden können, entdecken und desinfizieren lassen.

Dr.Web verwendet die Technologie Origins Tracing™ for Android, mit der schädliche Programme auf Android-Geräten rechtzeitig erkannt werden. Es ist die einzigartige Technologie zur Erkennung böswilliger Programme für Android-Plattformen. Diese Technologie sorgt dafür, dass neue Virenfamilien aufgrund der schon bestehenden Kenntnisse über herkömmliche Bedrohungen entdeckt werden können. Mit Origins Tracing for Android lassen sich sowohl neu kompilierte Viren wie Android.SMSSend oder Android.MobileSpy, als auch die mit Android.ADRD, Android.Geinimi oder Android.DreamExploit infizierten Anwendungen, erkennen. Die mit Hilfe von Origins Tracing for Android entdeckten Bedrohungen erhalten den Namen Android.VirusName.origin.

In diesem Handbuch finden Nutzer mobiler Android-Geräte detaillierte Informationen rund um die Installation und Konfiguration von **Dr.Web** sowie Hauptfunktionen der App.

Symbole und Hervorhebungen

In der Anleitung werden folgende Bezeichnungen verwendet:

Symbol/Hervorhebung	Erläuterung
Fette Schrift	Elemente der grafischen Benutzeroberfläche und Beispiele für Eingaben, die exakt, wie im Handbuch beschrieben, durchgeführt werden müssen.
Fette grüne Schrift	Namen von Doctor Web Produkten oder Komponenten.
<u>Grüne unterstrichene Schrift</u>	Querverweise auf eine Stelle im Handbuch oder Links auf Webseiten.
<i>Kursiv</i>	Kursivformatierung wird zur Darstellung von Begriffen oder von variablen Platzhaltern verwendet, für die der Benutzer spezifische Werte eingeben muss. Bei Eingaben in der Befehlszeile wird die Kursivformatierung zur Darstellung von Parameterwerten verwendet.
GROSSBUCHSTABEN	Bezeichnungen der Tastaturtasten.
	Wichtiger Hinweis bzw. wichtige Warnung vor potentiell gefährlichen Situationen oder möglichen Fehlern.

Hauptfunktionen der App

Dr.Web ist eine zuverlässige Antivirenlösung für mobile Geräten unter Android. Die Anwendung realisiert folgende Funktionen:

- Permanenter Echtzeitschutz des Dateisystems (Prüfung der zu speichernden Dateien, zu installierenden Programme u a.m.)
- Alle Dateien des Systems bzw. einzelne Dateien und Ordner auf Anforderung des Benutzers scannen
- Archive scannen
- Auf Speicherkarte scannen
- Windows-Autostart-Dateien entdecken



- Bedrohungen in .lnk-Dateien (durch **Dr.Web** als **Exploit.Cpllnk** definiert) entdecken
- Entdeckte Bedrohungen löschen bzw. in die Quarantäne verschieben
- Das Gerät bei seiner Blockierung durch Erpresser-Software freigeben
- Eingehende Anrufe und SMS-Nachrichten aufgrund der voreingestellten bzw. benutzerdefinierten White- und Blacklists filtern
- **Dr.Web Virendatenbanken** über das Internet aktualisieren
- Erfassung der Statistiken über erkannte Bedrohungen und Aktionen der App sowie Protokollierung der Ereignisse
- Handy orten und sofort sperren, wenn es verloren geht oder gestohlen wird
- Vor unerwünschten Webinhalten bei Nutzung eines Standard-Android-Browsers sowie des Browsers Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser bzw. Boat Browser Mini schützen
- URL überprüfen und kürzen
- Überprüfung des Geräts auf sicherheitsrelevante Schwachstellen und Hilfe bei der Behebung aufgespürter Probleme
- Internetverbindungen überwachen, das Gerät vor unbefugtem Zugriff von außen schützen sowie dem Verlust wichtiger Daten im Netzwerk vorbeugen



Einige hier aufgeführte Funktionen sind nicht verfügbar für Geräte unter [Android TV](#). Weitere Informationen finden Sie unter [Dr.Web für Android TV](#).

Durch eine bequeme graphische Oberfläche lassen sich die Anwendungsparameter mit Rücksicht auf Bedürfnisse des Benutzers vollständig konfigurieren und ein optimales Schutzniveau für mobiles Endgeräte einstellen.

Dr.Web kann auch im Multi-Window Modus genutzt werden. In diesem Modus lassen sich mehrere Anwendungen in einzelnen Fenstern starten. Der Multi-Window Modus wird nur von Samsung Galaxy S III und höher sowie Samsung Galaxy Note 2 und höher unterstützt.

Systemanforderungen

Dr.Web setzt Android 4.0/4.1/4.2/4.3/4.4/5.0/5.1 voraus. **Dr.Web** kann auch auf Fernsehern, Mediaplayern und Spielekonsolen unter Android TV verwendet werden.

Außerdem benötigen Sie eine Internetverbindung, um Updates für Virendatenbanken herunterzuladen. Wenn Sie einen Tablet-PC verwenden, muss die Möglichkeit bestehen, eine SIM-Karte einzulegen und zu nutzen, damit Filtern der Nachrichten und **Dr.Web Diebstahlschutz** funktionieren. Darüber hinaus ist die Firewall nur auf den Geräten mit Android 4.0 oder höher verfügbar.



Bitte beachten Sie, dass kein korrekter Betrieb von **Dr.Web** bei Geräten mit der durch Benutzer veränderten Firmware bzw. mit Root-Zugriff (sogenannte gerootete Geräte) garantiert werden kann. Des Weiteren wird kein technischer Support für solche Geräte geleistet.

Standardmäßig wird die Anwendung im internen Speicher des Geräts installiert. Damit **Dr.Web**, vor allem der **Dr.Web Diebstahlschutz**, ordnungsgemäß funktionieren kann, sollten Sie die installierte App nicht auf einen externen Speicher verschieben.



Kapitel 2. Lizenzierung

Um **Dr.Web** verwenden zu können, brauchen Sie eine gültige Lizenz. Eine gültige Lizenz ermöglicht Ihnen, alle Funktionen des Produkts im Laufe ihrer Gültigkeitsdauer zu nutzen, und regelt die aus der Lizenzvereinbarung resultierenden Rechte des Benutzers.

Wenn Sie das Produkt vor dem Lizenzwerb testen wollen, können Sie den [Testzeitraum aktivieren](#). Die Demoversion bietet Ihnen die Möglichkeit, die Hauptkomponenten voll funktionsfähig zu testen. Sie kann aber nur innerhalb eines kurzen Zeitraums verwendet werden.

Wenn Sie bereits eine gültige Lizenz für **Dr.Web Security Space**, **Dr.Web Desktop Security Suite** oder beliebige **Dr.Web** Box-Produkte haben, können Sie diese Lizenz für **Dr.Web** verwenden.



Wenn Sie die App mit der unbefristeten Lizenz (**Dr.Web Anti-virus Life license**) über den Google Play Store kaufen und installieren wollen, wird die Lizenz automatisch bereitgestellt und registriert.

Im [Zentralschutz-Modus](#) wird die Lizenz automatisch vom Zentralschutz-Server heruntergeladen.

Die Aktivierung der [Lizenz](#) oder des [Testzeitraums](#) bzw. der Kauf der Lizenz erfolgt auf dem entsprechenden Bildschirm (s. [Abbildung 1a und 1b](#)), der beim ersten Start der App bzw. bei fehlender Lizenz angezeigt wird.

So rufen Sie den Lizenzierungsbildschirm auf

1. Wählen Sie im Menü der App den Punkt **Über das Programm**. Wenn Sie ein Gerät unter [Android TV](#) haben, wechseln Sie auf dem Hauptbildschirm zu **Über das Programm**.
2. Tippen Sie auf **Lizenz aktualisieren**.



Abbildungen 1a und 1b. Lizenzierung



Lizenzschlüsseldatei

Rechte zur Nutzung von **Dr.Web** sind in einer speziellen Datei enthalten, die als *Lizenzschlüsseldatei* bezeichnet wird.

Die Lizenzschlüsseldatei hat die Erweiterung .KEY und enthält die folgenden Informationen:

- Zeitraum, in dem das Produkt genutzt werden kann.
- Liste verfügbarer Komponenten.
- Andere Einschränkungen.

Die Lizenzschlüsseldatei ist *gültig*, wenn alle die folgenden Bedingungen erfüllt sind:

- Die Lizenz ist noch nicht abgelaufen.
- Die Lizenz gilt für alle Module der App.
- Die Integrität der Lizenz ist nicht verletzt.

Wenn eine dieser Bedingungen nicht erfüllt ist, ist die Lizenzschlüsseldatei *ungültig*. In diesem Fall können schädliche Programme nicht mehr neutralisiert werden.



Die Bearbeitung der Schlüsseldatei bewirkt, dass sie nicht mehr gültig ist! Um eventuelle Beschädigung der Schlüsseldatei zu vermeiden, sollten Sie diese nicht in einem Texteditor öffnen.

Testzeitraum aktivieren

Wenn Sie die App testen wollen, können Sie einen 14-Tage-Testzeitraum aktivieren.

Die Vorgehensweise für die Aktivierung des Testzeitraums unterscheidet sich je nachdem, wie Sie **Dr.Web** auf Ihrem Gerät installiert haben.

Die App wurde über den Google Play Store installiert:

1. Tippen Sie auf dem Lizenzierungsbildschirm auf **Demoversion erhalten** (s. [Abbildung 1b](#)). Der Testzeitraum wird für die E-Mail-Adresse Ihres Google-Kontos aktiviert, das im Bereich **Demoversion erhalten** angezeigt wird. Wenn Sie mehrere Google-Konten haben, wird das erste Konto gewählt.
2. Wenn Sie bisher noch kein Google-Konto angelegt haben, wird das Fenster geöffnet, in dem Sie die E-Mail-Adresse eingeben müssen, für die der Testzeitraum aktiviert werden soll. Geben Sie eine gültige E-Mail-Adresse ein und tippen Sie auf **Lizenz erhalten**. Der Testzeitraum wird aktiviert.

Die App wurde von der Webseite von Doctor Web installiert:

1. Tippen Sie auf dem Lizenzierungsbildschirm auf **Demoversion erhalten** (s. [Abbildung 1a](#)).
2. Das Fenster wird geöffnet, in dem Sie die E-Mail-Adresse eingeben müssen, für die der Testzeitraum aktiviert werden soll. Geben Sie eine gültige E-Mail-Adresse ein.
3. Tippen Sie auf **Lizenz erhalten**. Der Testzeitraum wird aktiviert.

Lizenz kaufen

Die Vorgehensweise beim Kauf einer Lizenz unterscheidet sich je nachdem, wie Sie **Dr.Web** auf Ihrem Gerät installiert haben.



Wenn Sie die App auf einem Gerät unter **Android TV** installiert haben, können Sie keine Lizenz direkt über die App erwerben. Sie können aber eine Lizenz über den Google Play Store oder im [Onlineshop von Doctor Web](#) jederzeit kaufen.

Die App wurde über den Google Play Store installiert:

1. Tippen Sie auf dem Lizenzierungsbildschirm (s. [Abbildung 1b](#)) auf **Kaufen/Herunterladen**.
2. Wenn Sie bisher noch kein Google-Konto angelegt haben, wird das Fenster geöffnet, in dem Sie die E-Mail-Adresse eingeben müssen, die bei der Registrierung der Lizenz verwendet werden soll. Dadurch können Sie nachträglich Ihre Lizenz aktivieren, falls die App erneut oder auf einem anderen mobilen Gerät installiert werden muss. Geben Sie die gewünschte E-Mail-Adresse ein und tippen Sie auf **Lizenz erhalten**.
3. Wählen Sie auf dem Bildschirm **Lizenzkauf** eine der folgenden Varianten aus:
 - **Lizenz für 1 Jahr, Lizenz für 2 Jahre** oder **Lizenz für 1 Jahr ohne technischen Support**. Nachdem Sie die gewünschte Variante gewählt haben, wird das Fenster geöffnet, in dem Sie die Lizenz kaufen können. Die Lizenz wird automatisch aktiviert, sobald die Zahlung erfolgt ist. Wenn die Schlüsseldatei wegen eines technischen Problems beim Kaufvorgang nicht heruntergeladen werden kann, wenden Sie sich an den [technischen Support](#) von **Doctor Web**.
 - **Lizenz ohne zeitliche Begrenzung**. Wenn Sie die unbefristete Lizenz gewählt haben, wird das Fenster für den [Kauf und die Installation](#) von **Dr.Web Life license** im Google Play Store geöffnet. Wenn Sie **Dr.Web** bereits genutzt haben, werden Sie aufgefordert, dies zu deinstallieren. Tippen Sie auf **OK**, um den Löschvorgang zu bestätigen. Wenn Sie die Einstellungen der App auch weiterhin in **Dr.Web Antivirus Life license** verwenden wollen, [exportieren](#) Sie diese, bevor Sie mit der Deinstallation beginnen.



Wenn der **Dr.Web Diebstahlschutz** auf Ihrem Gerät aktiviert ist, muss das Häkchen bei **Dr.Web Security Space** in den Einstellungen des Geräts unter **Einstellungen – Sicherheit – Gerätedministratoren** vor dem Löschen von **Dr.Web** entfernt werden (Namen der Optionen können sich je nach Modell des Geräts bzw. Version des Betriebssystems unterscheiden). Das Gerät wird dann durch den **Dr.Web Diebstahlschutz** gesperrt. Geben Sie das für den **Dr.Web Diebstahlschutz** festgelegte Passwort ein, um den Löschvorgang fortzusetzen.

Die Lizenz wird automatisch aktiviert.

Die App wurde von der Webseite von Doctor Web installiert:

1. Tippen Sie auf dem Lizenzierungsbildschirm auf **Kaufen** (s. [Abbildung 1a](#)) oder tippen Sie auf den Link <http://estore.drweb.com/mobile>. Die Seite des Onlineshops von **Doctor Web** wird angezeigt.
2. Wählen Sie den gewünschten Lizenzzeitraum und die Anzahl der zu schützenden Geräte.
3. Tippen Sie auf **Kaufen**.

Nachdem die Bestellung erfolgt ist, wird die Seriennummer oder Lizenzschlüsseldatei an die bei der Bestellung angegebene E-Mail-Adresse gesendet. Alternativ kann die Seriennummer per SMS an die bei der Bestellung angegebene Mobiltelefonnummer gesendet werden. Sie müssen dann die [Seriennummer registrieren](#) bzw. die [Schlüsseldatei auf Ihr mobiles Gerät kopieren](#).

Lizenz aktivieren

Wenn Sie bereits eine gültige Lizenz für **Dr.Web Security Space**, **Dr.Web Desktop Security Suite** oder beliebige **Dr.Web** Box-Produkte haben, können Sie eine der unten aufgeführten Aktivierungsmethoden verwenden. Entscheidend ist dabei, wie Sie **Dr.Web** auf Ihrem Gerät installiert haben.

**Die App wurde über den Google Play Store installiert:**

- Wenn Sie eine Lizenz oder den Testzeitraum bereits aktiviert haben, tippen Sie auf dem Lizenzierungsbildschirm (s. [Abbildung 1b](#)) auf **Kaufen/Herunterladen**. Geben Sie bei Bedarf die E-Mail-Adresse ein, die Sie bei der Registrierung der Lizenz verwendet haben. Die auf diese E-Mail-Adresse registrierte Lizenz wird automatisch aktiviert.
- Wenn Sie bereits eine gültige Seriennummer haben, können Sie diese folgendermaßen registrieren:
 1. Tippen Sie auf dem Lizenzierungsbildschirm (s. [Abbildung 1b](#)) auf **Seriennummer eingeben**.



Die Seriennummer, die Sie zur Aktivierung des Testzeitraums eines der **Dr.Web** Produkte für Workstations erhalten haben, kann für **Dr.Web**, der über den Google Play Store installiert wurde, nicht verwendet werden. In diesem Fall müssen Sie zuerst den Testzeitraum für das **Dr.Web** Produkt auf einem Rechner aktivieren. Danach erhalten Sie die entsprechende Lizenzschlüsseldatei. Diese Datei kann dann auf Ihr mobiles Gerät **kopiert** werden. Anweisungen für die Verwendung der erhaltenen Lizenzschlüsseldatei auf einem mobilen Gerät werden an die bei der Aktivierung des Testzeitraums angegebene E-Mail-Adresse zugesendet.

2. Geben Sie die bestehende Seriennummer ein und tippen Sie auf **Lizenz erhalten**.

Die App wurde von der Webseite von Doctor Web installiert:

Sie können eine der folgenden Aktivierungsmethoden verwenden.

Seriennummer registrieren

1. Tippen Sie auf dem Lizenzierungsbildschirm (s. [Abbildung 1a](#)) auf **Lizenz aktivieren**.
2. Wählen Sie den Punkt **Seriennummer eingeben**.
3. Geben Sie die Seriennummer ein.
4. Wenn Sie diese Seriennummer noch nicht registriert haben, wird der Bildschirm angezeigt, auf dem Sie zur Aktivierung der Lizenz Ihre persönlichen Daten angeben müssen. Füllen Sie alle Felder aus.
5. Tippen Sie auf **Lizenz erhalten**.

Schlüsseldatei auf ein Gerät kopieren

1. Kopieren Sie Ihre Schlüsseldatei in den Ordner **Android/data/com.drweb/files** auf der SD-Karte.
2. Tippen Sie auf dem Lizenzierungsbildschirm (s. [Abbildung 1a](#)) auf **Lizenz aktivieren**.
3. Tippen Sie auf **Aus der Datei laden**. Tippen Sie im nächsten Fenster **Aus Datei kopieren** auf **OK**.
4. Die Schlüsseldatei wird installiert und kann anschließend verwendet werden. Das Fenster mit Informationen über die Lizenzlaufzeit wird geöffnet. Tippen Sie auf **OK**.



Eine Schlüsseldatei für **Dr.Web Security Space** oder **Dr.Web Desktop Security Suite** kann ebenfalls für **Dr.Web** verwendet werden, falls sie die Komponente DrWebGUI unterstützt.

So überprüfen Sie, ob eine Schlüsseldatei verwendet werden kann:

1. Öffnen Sie Ihre Schlüsseldatei in einem Text-Editor (z. B. im Microsoft Editor).
2. Überprüfen Sie, ob der Parameter Applications in der Gruppe [Key] den Wert DrWebGUI enthält. Wenn diese Komponente in der Liste vorhanden ist, kann diese Schlüsseldatei für **Dr.Web** verwendet werden.

Schlüsseldateien sind vor Bearbeitung geschützt. Die Bearbeitung der Schlüsseldatei macht sie ungültig. Um die Beschädigung der Datei zu vermeiden, sollten Sie diese nach dem Öffnen nicht in einem Text-Editor speichern.

Schlüsseldatei bei der Registrierung einer Seriennummer auf der Webseite von Doctor Web erhalten



1. Rufen Sie die Webseite auf, die in der beigefügten Registrierungskarte angegeben ist.
2. Geben Sie die Seriennummer an, die Sie beim Kauf von **Dr.Web Antivirus** erhalten haben.
3. Geben Sie alle erforderlichen Daten zum Käufer an.
4. Ihre Schlüsseldatei wird an die von Ihnen angegebene E-Mail-Adresse als ZIP-Archiv zugesendet. Dieses Archiv enthält eine Datei mit der KEY-Erweiterung.
5. Extrahieren Sie diese Schlüsseldatei auf einem Rechner. [Kopieren](#) Sie dann diese Datei auf Ihr Gerät.

Lizenz verlängern

In manchen Fällen, z. B. bei Lizenzablauf, kann es erforderlich sein, die bereits vorhandene und im System registrierte Lizenzschlüsseldatei zu ersetzen. **Dr.Web** unterstützt die "on the fly"-Aktualisierung der Schlüsseldatei. Dabei brauchen Sie, die Schlüsseldatei nicht neu zu installieren bzw. ihre Nutzung zu unterbrechen.

Informationen zur Lizenz

Um Informationen zur genutzten Lizenz einsehen:

- **Unter Android:** Rufen Sie auf dem Hauptbildschirm des Programms (s. [Abbildung 2](#)) das App-Menü auf und wählen Sie den Punkt **Über das Programm**.
- **Unter Android TV:** Wechseln Sie auf dem Hauptbildschirm (s. [Abbildung 20](#)) zu **Über das Programm**.

Im geöffneten Bildschirm können Sie die folgenden Informationen zur Lizenz einsehen:

- Name des Lizenzinhabers
- Registrierungs- sowie Ablaufdatum der Lizenz

Benachrichtigungen konfigurieren

Sie können die Benachrichtigungen über eine bald ablaufende Lizenz aktivieren/deaktivieren. Dazu navigieren Sie zu **Benachrichtigungen** in dem Bereich Lizenz in den Einstellungen von **Dr.Web** (s. [Abbildung 6](#)).

Lizenz aktualisieren

Für die Aktualisierung der Lizenz müssen Sie eine neue Schlüsseldatei [erhalten](#) oder [registrieren](#).

Sie können auch eine neue Lizenz erwerben bzw. die aktuelle Lizenz in Ihrem [persönlichen Bereich](#) auf der offiziellen Webseite von **Doctor Web** verlängern. Um auf diese Seite zu gelangen, wählen Sie im App-Menü den Punkt **Über das Programm** aus und tippen Sie auf den Link **Mein Dr.Web**.



Kapitel 3. Installation und Deinstallation

Dr.Web kann direkt über den Google Play erworben und installiert werden. Alternativ können Sie die Installationsdatei auf Ihr mobiles Gerät kopieren und anschließend starten. Um die App zu installieren, können Sie auch ein Synchronisierungsprogramm verwenden.

Die App kann über den Google Play Store bzw. mit Android-Bordmitteln deinstalliert werden.

App installieren

Dr.Web kann über Google Play sowie durch Ausführen der Installationsdatei auf dem Gerät bzw. mit Hilfe eines Programms zum Synchronisieren mit dem PC installiert werden.

Anwendung über Google Play installieren

1. Öffnen Sie Google Play und finden Sie **Dr.Web**. Tippen Sie auf **Installieren oder Kaufen** je nach der Version der Anwendung.



Wenn **Dr.Web** im Google Play Store nicht zu finden ist, erfüllt das mobile Endgerät die minimalen Systemanforderungen nicht.

2. Wenn Sie die App mit der unbefristeten Lizenz installieren (**Dr.Web Life license**), öffnet es sich der Bildschirm mit Zahlungsoptionen.
3. Nachdem die Zahlung geleistet wurde, öffnen sich die Informationen zu Zugriffsrechten, welche durch die Anwendung benötigt werden. Um richtig zu funktionieren, erfordert die App Zugriff auf folgende Daten:
 - bei der Installation der Antivirensoftware **Dr.Web** für einen kostenlosen Testzeitraum (14 Tage) wird der Zugriff auf die In-App-Kauf-Funktion für den Lizenzerwerb benötigt, nachdem der Testzeitraum abgelaufen ist;
 - zum Registrieren der Anwendung und Aktivieren der Lizenz wird ein Internetzugriff sowie Zugriff auf die Liste der Google-Konten auf dem Gerät benötigt;
 - damit der Datei-Wächter **SpIDer Guard** und der Scanner funktionieren, wird Zugriff auf den Gerät-Speicher, die Daten der Anwendungen und die SD-Karte sowie eine Möglichkeit zum Lesen und Schreiben von Daten benötigt;
 - zum Filtern von Anrufen und SMS-Nachrichten benötigt man Zugriff auf Sende- und Empfangsfunktionen sowie eine Möglichkeit, die Kontaktliste und den Anruf- und SMS-Nachrichtenverlauf zu lesen, sowie den Signalmodus zu ändern (um den Ton auszuschalten, wenn der Anruf gesperrt wird);
 - damit der **Dr.Web Diebstahlschutz** funktioniert, wird Zugriff auf SMS-Sendefunktionen (um Nachrichten von **Dr.Web Diebstahlschutz** über den SIM-Kartenwechsel sowie Antworten auf gesendete Befehle zu senden), Ortungsfunktionen, Funktionen zur GPS- und Wi-Fi-Verwaltung sowie eine Möglichkeit, alle persönlichen Daten auf dem Gerät zu löschen (wenn ein entsprechender Befehl empfangen wird), benötigt;
 - zur Funktion des **Cloud Checker** URL-Filters wird Zugriff auf Verlauf und Lesezeichen der unterstützten Browser benötigt;
 - zur Verwendung des unverankerten Fensters mit Informationen zum aktuellen Datenverkehr muss für Benutzeroberflächenelemente die Anzeige im Vordergrund aktiviert werden;
 - zur Aktualisierung von Virendatenbanken wird ein Internetzugriff sowie Zugriff auf die Netzwerkeinstellungen des Geräts benötigt.

Tippen Sie auf **OK**.



4. Die Anwendung wird automatisch installiert.

Um die Anwendung ohne Verwendung von Google Play zu installieren, müssen Sie eine solche Installationsart erlauben. Öffnen Sie hierzu den Abschnitt **Einstellungen** -> **Sicherheit** und setzen Sie ein Häkchen bei **Unbekannte Herkunft**. Die Installationsdatei **Dr.Web** kann von der Webseite von **Doctor Web** unter <http://download.drweb-av.de/android> heruntergeladen werden.

Installationsdatei auf einem Gerät starten

1. Kopieren Sie die Installationsdatei auf die SD-Karte.



Zur Suche und Ausführung der Datei auf dem Endgerät wird ein Datei-Browser benötigt.

2. Verwenden Sie den Datei-Browser, um die Installationsdatei zu finden und auszuführen.
3. Die Anwendung wird automatisch installiert.

Installation mit Hilfe des Programms zum Synchronisieren des mobilen Endgeräts mit dem PC (z.B. HTC Sync™ u. a.)

1. Synchronisieren Sie Ihr mobiles Gerät mit dem PC.
2. Starten Sie den Anwendungsinstallations-Assistenten, der zum Umfang der Synchronisationssoftware gehört.
3. Geben Sie den Pfad der Installationsdatei auf dem Rechner an und folgen Sie den Anweisungen des Installationsassistenten.
4. Die Anwendung wird auf das mobile Gerät übertragen. Somit können Sie die Informationen dazu einsehen und die Installation akzeptieren. Nach der Bestätigung wird die Anwendung automatisch installiert.
5. Beenden Sie den Installationsassistenten der Synchronisationssoftware.

Dr.Web ist installiert und bereit zur Nutzung bereit. Wenn die Anwendung ohne Verwendung von Google Play installiert wird, müssen Sie die [Lizenz registrieren](#), um diese Anwendung nutzen zu können. Wenn Sie keine gültige Schlüsseldatei haben, nutzen Sie das [Verfahren zum Erhalten der Schlüsseldatei](#).



Standardmäßig wird die Anwendung im internen Speicher des Geräts installiert. Damit **Dr.Web**, vor allem der **Dr.Web Diebstahlschutz**, ordnungsgemäß funktionieren kann, sollten Sie die installierte App nicht auf einen externen Speicher verschieben.

App deinstallieren und aktualisieren

Die App lässt sich über den Google Play Store auf eine neuere Version aktualisieren bzw. deinstallieren. Alternativ können Sie die App mit Android-Bordmitteln ohne Verbindung zum Internet deinstallieren.



Wenn Sie auf Ihrem Gerät den **Dr.Web Diebstahlschutz** aktiviert haben, müssen Sie vor der Deinstallation in den Einstellungen unter **Sicherheit – Geräteadministratoren** das Häkchen bei **Dr.Web Security Space** entfernen (die Namen der Optionen können sich je nach Modell des Geräts bzw. Version des Android-Betriebssystems unterscheiden).

App über den Google Play Store deinstallieren und aktualisieren

1. Öffnen Sie den Google Play Store und wählen Sie den Punkt **Meine Downloads** oder **Meine Apps** (je nach verwendeter Version des Betriebssystems) aus.
2. Tippen Sie in der Liste der auf dem Gerät installierten Anwendungen auf das Symbol von **Dr.Web**



Wenn **Dr.Web** ohne Verwendung von Google Play installiert wurde, kann die Anwendung im Bereich **Meine Downloads** fehlen. In diesem Fall können Sie das Programm mit Betriebssystemmitteln löschen.

3. Tippen Sie auf dem Bildschirm mit Informationen zur Anwendung auf **Aktualisieren**, um eine neue Version zu installieren, bzw. auf **Deinstallieren**, um die App zu deinstallieren.
4. Bestätigen Sie die Aktualisierung/Deinstallation der Anwendung:
 - Die Vorgehensweise für die Aktualisierung der App ist identisch mit der unter App installieren beschriebenen.
 - Bei der Deinstallation der App müssen Sie einen Grund für die Deinstallation angeben und dann auf **OK** tippen. Die App wird deinstalliert.

App ohne Internetverbindung deinstallieren

1. Wechseln Sie zu **Einstellungen** -> **Apps**.
2. Tippen Sie in der Liste der auf dem Gerät installierten Anwendungen auf das Symbol von **Dr.Web**

3. Tippen Sie auf dem Bildschirm mit Informationen zur Anwendung auf **Deinstallieren**. Die App wird deinstalliert.
4. Nachdem die Deinstallation beendet ist, tippen Sie auf **OK**, um zur Liste der installierten Anwendungen zurück zu wechseln.



Die Quarantäne und das gespeicherte Ereignisprotokoll werden standardmäßig nicht gelöscht. Gegebenenfalls können Sie diese manuell aus dem Ordner `Android/data/com.drweb/files` auf der SD-Karte löschen.

Verfügbarkeit einer neuen App-Version überprüfen

Wenn Sie **Dr.Web** von der Webseite von **Doctor Web** heruntergeladen und installiert haben, können Sie die App so konfigurieren, dass die Verfügbarkeit neuer App-Versionen bei jeder Aktualisierung der Virendatenbanken automatisch überprüft wird. Setzen Sie hierzu in den Einstellungen des Updates der App das Häkchen bei **Neue Version der Anwendung**. Erscheint eine neue Anwendungsversion, werden Sie darüber standardmäßig informiert und können die neue Version schnell herunterladen und installieren.



Kapitel 4. Mit der Arbeit beginnen

Dieser Abschnitt beschreibt das Verfahren zum Starten und Beenden von **Dr.Web** sowie die Benutzeroberfläche der Anwendung.

App starten und beenden

App starten

So starten Sie **Dr.Web**

- **Unter Android:** Öffnen Sie den Bildschirm **Apps** und tippen Sie auf das Symbol von **Dr.Web** .
- **Unter Android TV:** Wechseln Sie zu **Apps** und wählen Sie in der Liste der verfügbaren Apps **Dr.Web** aus.

Beim ersten Start der App öffnet sich die Lizenzvereinbarung, die Sie akzeptieren müssen. In diesem Fenster können Sie sich auch mit Informationen über das Programm zur Verbesserung der Software-Qualität vertraut machen sowie Ihre Teilnahme daran akzeptieren, indem Sie sich mit einem automatischen Versand nicht-personenbezogener Daten zu entdeckten Bedrohungen und besuchten Websites an Server von **Doctor Web** und Google einverstanden erklären. Sie können zu jeder Zeit auf Versand dieser Statistik in den [Einstellungen](#) der Anwendung verzichten. Dafür wählen Sie das Häkchen bei **Statistik senden** im Bereich **Allgemein** ab.



Wenn **Dr.Web** mithilfe der vom [Administrator des Antivirus-Netzwerks](#) des Unternehmens bereitgestellten Installationsdatei installiert wurde, wird die Lizenzvereinbarung nicht angezeigt.

App beenden

Um die Anwendung zu beenden, tippen Sie auf die **Home**-Schaltfläche .

Zum wiederholten Start der Anwendung können Sie auf das Symbol von **Dr.Web**  im Bereich für zuletzt gestartete Anwendungen tippen.

Beim ersten Starten öffnet sich **Dr.Web** auf dem Hauptbildschirm. Beim wiederholten Starten öffnet sich das Programm in dem Bereich, der zuletzt aktiv war, als das Programm beendet wurde.

Oberfläche

Der Hauptbildschirm von **Dr.Web** (s. [Abbildung 2](#)) enthält Informationen zum aktuellen Sicherheitsstand des Systems und lässt auf folgende Funktionen der App zugreifen:

- **SpIDer Guard** – damit lässt sich der permanente Virenschutz aktivieren/deaktivieren.
- **Anruf- und Nachrichtenfilter** – ermöglicht es, den Filterungsmodus zu wählen sowie die Listen der gesperrten Anrufe und Nachrichten einzusehen.



Auf mobilen Geräten ohne SIM-Karten-Slot fehlen der Anruf- und SMS-Filter und der **Dr.Web Diebstahlschutz**. Aus diesem Grund werden diese Abschnitte auf dem Hauptbildschirm nicht angezeigt. Auf Geräten unter [Android TV](#) ist die **Dr.Web Firewall** nicht verfügbar.

- **Scanner** – überprüft das System auf Anforderung des Benutzers (3 Prüfungsarten stehen zur Verfügung: schnell, vollständig und benutzerdefiniert).
- **Update** – enthält Informationen zum letzten Update und ermöglicht, die App bei Bedarf zu

aktualisieren.

- **Diebstahlschutz** – ermöglicht es, die Funktionen vom **Dr.Web Diebstahlschutz** zu konfigurieren.
- **Cloud Checker** – damit lässt sich der URL-Filter zur Einschränkung des Benutzerzugriffs auf die Webinhalte konfigurieren.
- **Firewall** – ermöglicht es, die Überwachung der Internetverbindungen und die Datenübertragung im Netzwerk zu konfigurieren.
- **Security Auditor** – ermöglicht es, das System zu analysieren und erkannte Sicherheitsprobleme und -lücken zu beseitigen.

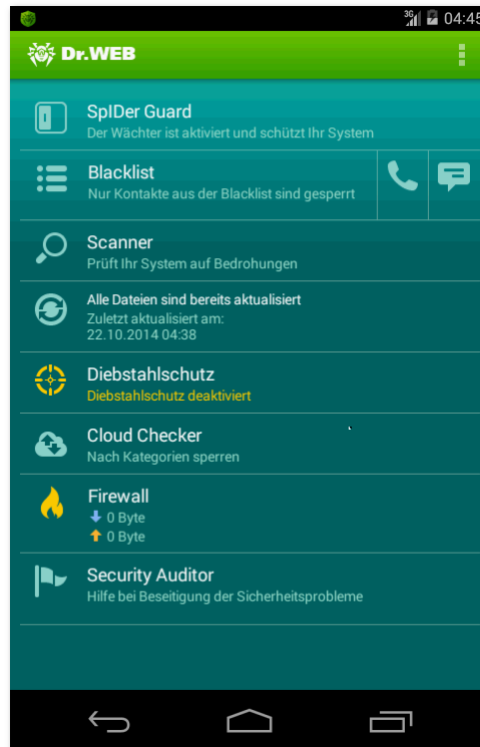


Abbildung 2. Hauptbildschirm der App

Zugriff auf das Menü und Navigation innerhalb der App

Auf den Anwendungsbildschirmen mit zusätzlichen Optionen wird das Menü mit einer Taste oben in der rechten Bildschirmcke aufgerufen. Um zum Hauptbildschirm zurückzukehren, tippen Sie auf das Logo der App in der oberen linken Ecke des Bildschirms.

Über das Menü auf dem Hauptbildschirm können Sie zu den Einstellungen der App wechseln, die [Quarantäne](#) öffnen und [Statistiken](#) zur App abrufen, Informationen über die App anzeigen.

Auf dem Bildschirm mit den Informationen über die App stehen Ihnen Informationen zur App-Version, zum Lizenzinhaber sowie Aktivierungs- und Ablaufdatum der Lizenz zur Verfügung. In diesem Bereich finden Sie auch Links zur offiziellen Webseite von **Doctor Web**, zu Ihrem [persönlichen Bereich](#) auf der offiziellen Webseite sowie zu unseren Profilen in den sozialen Netzwerken Twitter, Facebook, Instagram und Youtube. Wenn sich **Dr.Web** im Zentralschutz-Modus befindet und im Rahmen des Services **Dr.Web AV-Desk** verwendet wird, wird auf diesem Bildschirm auch das Abo-Ablaufdatum oder das Datum angezeigt, ab dem der Service für dieses Gerät (diese Workstation) eingestellt wurde.



Das Menü ist nicht verfügbar auf Geräten unter [Android TV](#). Informationen zur App-Version, zum Lizenzinhaber sowie Aktivierungs- und Ablaufdatum der Lizenz können Sie über den Menüpunkt **Über das Programm** auf dem Hauptbildschirm anzeigen lassen.

Widgets

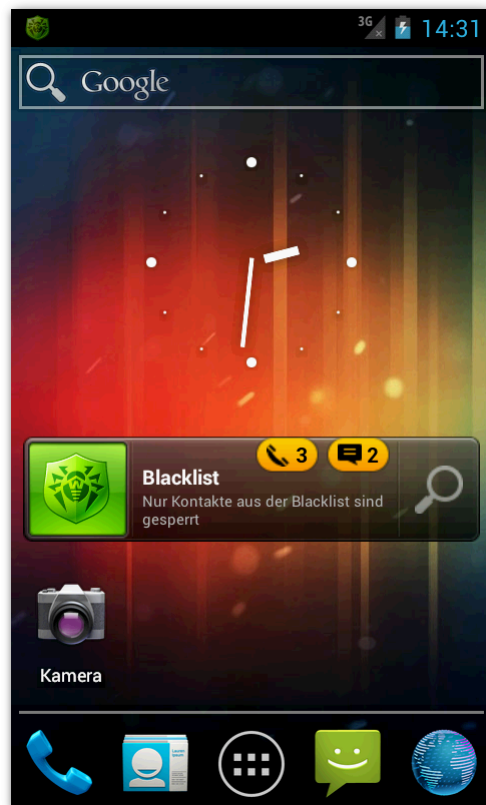
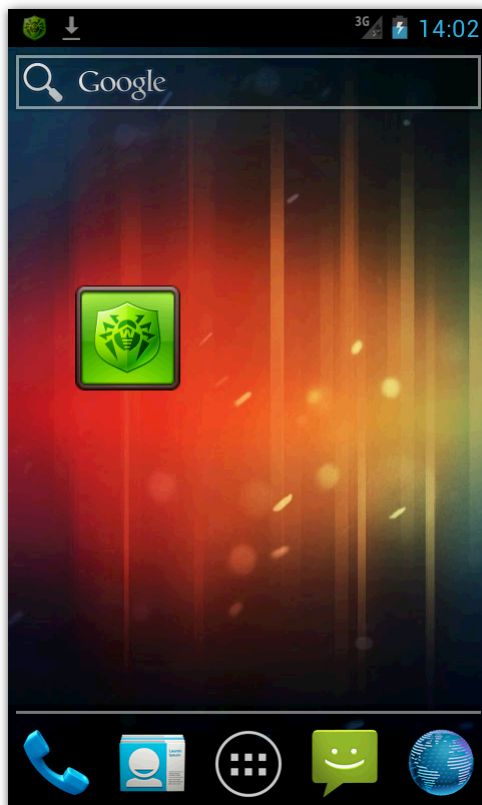
Damit die Nutzung von **Dr.Web** bequemer ist, können Sie spezielle Widgets auf den **Startbildschirm** Ihres Geräts bringen. Durch diese Widgets lassen sich die Hauptfunktionen der App leicht verwalten.



Widgets sind nicht verfügbar auf Geräten unter [Android TV](#).

Widget hinzufügen

1. Die Widgets der App können mithilfe von Standard-Werkzeugen Ihres Betriebssystems hinzugefügt werden. Öffnen Sie die Liste von Widgets, die auf Ihrem Gerät hinzugefügt werden können.
2. In der Liste der verfügbaren Widgets wählen Sie eines der Widgets von **Dr.Web**:
 - **Dr.Web 1x1 (klein)** – zeigt den aktuellen Schutzstatus und ermöglicht die Aktivierung/Deaktivierung von **SpIDer Guard** (s. [Abbildung 3](#)).
 - **Dr.Web 4x1 (mittelgroß)** – zeigt den aktuellen Schutzstatus, das aktuelle Filterprofil, die Anzahl der gesperrten Anrufe und Nachrichten und ermöglicht die Aktivierung/Deaktivierung von **SpIDer Guard**, sowie den Übergang zum Scan-Bildschirm (s. [Abbildung 4](#)).



Abbildungen 3 und 4. Dr.Web Widgets

Benachrichtigungen

Um schnell auf die Grundfunktionen von **Dr.Web** schnell zuzugreifen, können Sie die spezielle Benachrichtigungsleiste oben auf dem Bildschirm nutzen (s. [Abbildung 5](#)). Um diese Leiste zu aktivieren/deaktivieren, navigieren Sie zur **Benachrichtigungsleiste** im Bereich **Allgemein**

(s. [Abbildung 6](#)).



Die Benachrichtigungsleiste ist nicht verfügbar auf Geräten unter [Android TV](#).

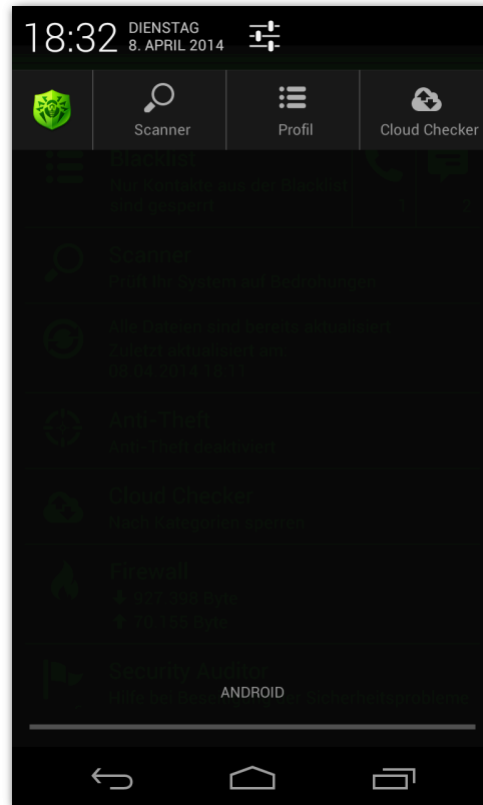


Abbildung 5. Benachrichtigungsleiste

Die Benachrichtigungsleiste bietet folgende Möglichkeiten:

- Zum Bildschirm von **Dr.Web** wechseln. Tippen Sie dazu auf das **Dr.Web**-Symbol.
- Schnelles, vollständiges bzw. benutzerdefiniertes Scannen starten. Wählen Sie dazu die Option **Scanner** und den entsprechenden Scanvorgang aus.
- Filterprofil für Anrufe und Nachrichten anhand der Option **Profil** wählen.



Wenn Ihr Gerät keine SIM-Karten unterstützt, wird die Option **Downloads** anstatt der Option **Profil** in der Benachrichtigungsleiste angezeigt. Diese Option ermöglicht es, dass die auf das Gerät heruntergeladenen Objekte durchsucht werden.

Wenn sich **Dr.Web** im **Zentralschutz-Modus** befindet und Sie keine Berechtigung zum Ändern der Einstellungen des Anruf- und SMS-Filters oder von **Cloud Checker** haben, werden die Optionen **Profil** und/oder **Cloud Checker** auf der Benachrichtigungsleiste nicht angezeigt.

- Zum Einstellungsbildschirm des URL-Filters anhand der Option **Cloud Checker** wechseln.



Sollten Bedrohungen erkannt werden, ändern sich die entsprechenden Symbole in der Benachrichtigungsleiste:

-  – wenn die Bedrohungen durch den Scanner erkannt wurden;
-  – wenn die Bedrohungen durch den Datei-Wächter **SpIDer Guard** erkannt wurden.



Unter Android 5.0 und höher wird die Benachrichtigung über eine Bedrohung in der Benachrichtigungsleiste solange über alle laufenden Anwendungen eingeblendet, bis Sie eine Aktion für die Bedrohung durchführen.

Mein Dr.Web

Nutzen Sie den Online-Service **Mein Dr.Web**, um Ihren persönlichen Bereich auf der Webseite von **Doctor Web** zu besuchen. Auf dieser Internetseite finden Sie Informationen zu Ihrer Lizenz (Gültigkeitsdauer, Seriennummer). Weiterhin können Sie die aktuelle Lizenz verlängern, das Datum und die Uhrzeit des letzten Updates sowie die Anzahl der Signaturen in den Virendatenbanken einsehen, Nachrichten und Sonderangebote erhalten, eine Frage an den technischen Support stellen u. v. m.

Um diese Webseite zu öffnen, rufen Sie das Anwendungsmenü auf dem Hauptbildschirm auf (s. Abbildung 2) und wählen Sie **Über das Programm**. Tippen Sie im geöffneten Bildschirm auf **Mein Dr.Web**.



Kapitel 5. Programmfunktionen und -einstellungen

Dieser Abschnitt beschreibt die grundsätzlichen Möglichkeiten von **Dr.Web**, mit denen sich die Virenprüfung, der Anruf- und Nachrichtenfilter, die Funktion vom **Dr.Web Diebstahlschutz** und der URL-Filter konfigurieren sowie der Schutz des Geräts auf solche Weise einrichten lässt.



Die Einstellungen der App sind nicht verfügbar auf Geräten unter **Android TV**.

Um auf den Einstellungsbildschirm der App zu gelangen (s. **Abbildung 6**), öffnen Sie auf dem Hauptbildschirm der App das Menü und wählen Sie dann **Einstellungen**.

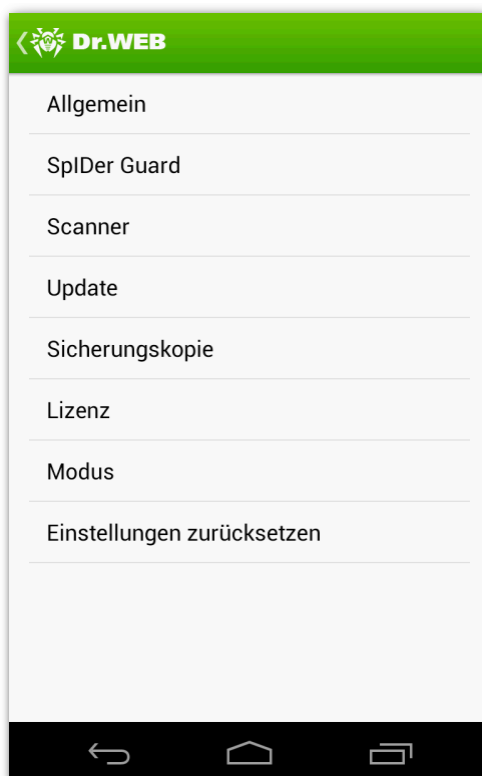


Abbildung 6. Einstellungen der App



Beim aktivierten **Dr.Web Diebstahlschutz** sind einige Bereiche der App (**Einstellungen zurücksetzen**, **Sicherungskopie** und **Modus**) passwortgeschützt. Um ihre Einstellungen ändern zu können, müssen Sie das Passwort des **Dr.Web Diebstahlschutzes** angeben.

Einstellungen zurücksetzen

Benutzerdefinierte Einstellungen, darunter auch die des **Dr.Web Diebstahlschutzes**, der **Dr.Web Firewall** und von **Cloud Checker**, können jederzeit auf Standardeinstellungen zurückgesetzt werden. Dafür müssen Sie wie folgt vorgehen:

1. Wählen Sie im Einstellungsbildschirm (s. **Abbildung 6**) im Bereich **Einstellungen zurücksetzen** den Punkt **Standardeinstellungen wiederherstellen** aus.
2. Bestätigen Sie die Wiederherstellung von Default-Einstellungen.

Einstellungen importieren und exportieren



Es ist möglich, alle aktuellen Einstellungen der Anwendung in einer Datei auf der SD-Karte zu speichern. Gegebenenfalls (z. B. wenn **Dr.Web** neu installiert bzw. auf einem anderen Gerät verwendet wird) können Sie diese Einstellungen später aus der Datei laden.

1. Um aktuelle Konfiguration zu speichern, wählen Sie den Punkt **Exportieren von Daten** im Bereich **Sicherungskopie** im Einstellungsbildschirm (s. [Abbildung 6](#)) aus. Geben Sie im geöffneten Fenster das Passwort für die Konfigurationsdatei ein und tippen Sie auf **OK**. Alle Einstellungen und Daten der App werden in der Datei `Android/data/com.drweb/files/DrWebPro.bkp` auf der SD-Karte gespeichert.
2. Um die Einstellungen aus der Datei zu laden, wählen Sie den Punkt **Importieren von Daten** im Bereich **Sicherungskopie** auf dem Einstellungsbildschirm (s. [Abbildung 6](#)) aus. Bestätigen Sie das Herunterladen von Parametern aus der Datei und geben Sie das Passwort der Konfigurationsdatei ein. Alle aktuellen Einstellungen werden gelöscht und durch die aus der Datei heruntergeladenen Einstellungen ersetzt.

Virenschutz

Die Hauptfunktion, die durch **Dr.Web** realisiert wird, ist eine [permanente Überprüfung](#) des Dateisystems in Echtzeit. Darüber hinaus scannt **Dr.Web** das System [auf Anforderung des Benutzers](#). Wenn Sicherheitsbedrohungen entdeckt werden, werden die durch Benutzer ausgewählten [Aktionen](#) dafür verwendet.

Permanenter Virenschutz

Die permanente Echtzeit-Prüfung des Dateisystems erfolgt mithilfe von **SpIDer Guard**. Er überprüft alle Dateien, beim Versuch sie im Speicher des mobilen Geräts zu speichern. Dadurch kann das System vor Sicherheitsbedrohungen effizienter geschützt werden.



Im [Zentralschutz-Modus](#) können die Einstellungen der Komponente **SpIDer Guard** entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein.

Permanenten Schutz aktivieren

Beim ersten Starten von **Dr.Web** wird der permanente Schutz automatisch nach Akzeptieren der Lizenzvereinbarung aktiviert. Um den Schutz zu deaktivieren bzw. erneut zu aktivieren, tippen Sie auf dem Hauptbildschirm der App auf **SpIDer Guard**.

Beim Aktivieren beginnt der Wächter, Ihr System zu schützen. Er funktioniert weiter unabhängig davon, ob die Anwendung gestartet ist oder nicht. Wenn eine Sicherheitsbedrohung erkannt wird, erscheint das Warnsymbol  (für Android 5.0 und höher – ) und eine Benachrichtigung über die erkannte Bedrohung in der Statusleiste des Geräts. Im Benachrichtigungen-Bereich können Sie die Informationen zu Anzahl entdeckter Bedrohungen einsehen und die Liste der Bedrohungen öffnen, um [Aktionen](#) zur deren Neutralisierung auszuführen.



Der Dateiwächter wird gestoppt, wenn der Speicher Ihres Geräts im integrierten Task-Manager komplett geleert wird. In diesem Fall müssen Sie **Dr.Web** wiederholt öffnen, um ständigen Virenschutz wiederherzustellen.

Einstellungen von SpIDer Guard

Für den Zugriff auf die Einstellungen von **Dr.Web** auf dem Hauptbildschirm des Programms rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**. Um den Dateiwächter zu konfigurieren, gehen Sie im Einstellungsbildschirm (s. [Abbildung 6](#)) wie folgt vor:

- Um die Prüfung von Dateien in Archiven zu aktivieren, setzen Sie ein Häkchen bei **Dateien in Archiven** im Bereich **SpIDer Guard**.



Standardmäßig ist die Archivprüfung deaktiviert. Durch die Aktivierung der Archivprüfung kann die Operationsgeschwindigkeit des Betriebssystems beschränkt und die Batterielaufzeit reduziert werden. Dabei beeinflusst die Deaktivierung der Archivprüfung den Schutzstatus nicht, da die Installationsdateien für Android-Betriebssysteme (.apk) durch den Dateiwächter überprüft werden, unabhängig davon, welcher Wert für diesen Parameter festgelegt wurde.

- Um die Prüfung der SD-Karte bei jedem Anschließen an das Gerät zu aktivieren, setzen Sie ein Häkchen bei **SD-Karte anschließen** im Bereich **SpIDer Guard**.
- Um die Überprüfung des Systems auf Adware und PUAs (darunter auch Dialer und Scherzprogramme) zu aktivieren/deaktivieren, wählen Sie den Punkt **Optionen** im Bereich **SpIDer Guard** und setzen/wählen Sie das Häkchen bei **Adware** und **Riskware** ab.
- Um die SD-Karte auf Windows-Autostart-Dateien zu überprüfen, setzen Sie ein Häkchen bei **Autorun-Dateien** im Bereich **Allgemein**. Diese Einstellung wird auch beim Scannen auf Anforderung des Benutzers verwendet.
- Um die Anzeige des App-Symbols  (für Android 5.0 und höher – ) in der Statusleiste nach der Aktivierung des Wächters zu aktivieren, setzen Sie im Bereich **Allgemein** ein Häkchen bei **Dr.Web Icon**.

Statistik

Die App protokolliert Ereignisse, die mit dem Betrieb von **SpIDer Guard** (darunter Informationen über die Aktivierung/Deaktivierung, Scan-Ergebnisse und erkannten Sicherheitsbedrohungen) verbunden sind. Aktionen der App, insbesondere von **SpIDer Guard**, werden im Bereich **Aktionen** auf der Registerkarte **Statistik** nach Datum sortiert angezeigt.

Überprüfung auf Anforderung des Benutzers

Das System wird auf Anforderung des Benutzers mit Hilfe einer speziellen Komponente – eines Scanners – überprüft. Der **Dr.Web** Scanner ermöglicht das schnelle oder vollständige Scannen des Dateisystems sowie die Überprüfung einzelner Dateien und Ordner.



Im **Zentralschutz-Modus** können die Einstellungen des Scanners entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein. Scanvorgänge können ebenfalls nach dem am Zentralschutz-Server festgelegten Zeitplan gestartet werden.

Scannen

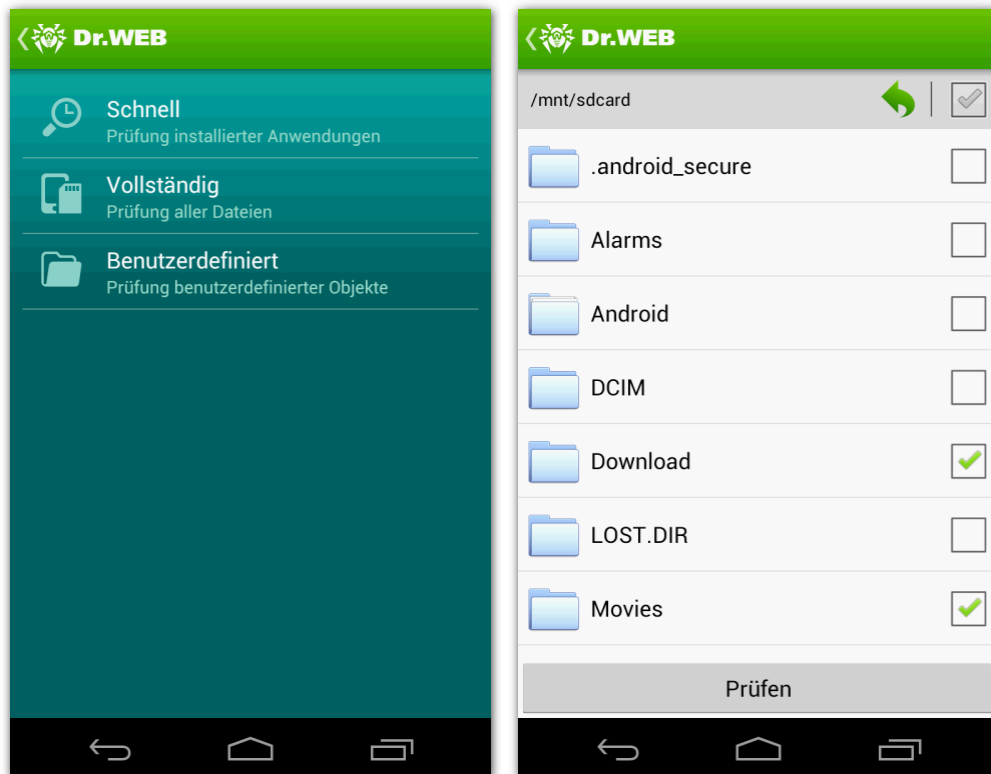
Um das System zu scannen, tippen Sie im Hauptbildschirm auf **Scanner** und führen Sie im geöffneten Fenster (s. [Abbildung 7](#)) eine der folgenden Aktionen durch:

- Um das Scannen installierter Anwendungen zu starten, wählen Sie den Punkt **Schnell**.
- Um das Scannen aller Dateien im System zu starten, wählen Sie den Punkt **Vollständig**.



- Um einzelne Dateien und Ordner zu überprüfen, wählen Sie den Punkt **Benutzerdefiniert**. In der geöffneten Liste mit Objekten des Dateisystems wählen Sie erforderliche Objekte aus (s. [Abbildung 8](#)) und tippen Sie auf **Prüfen**. Für die Auswahl der Objekte in der Liste können Sie die Optionen benutzen, die sich rechts über der Liste befinden und alle Elemente der Liste wählen bzw. auf die nächste höhere Ebene wechseln, um zwischen den Ordnern zu navigieren.

Nachdem das Scannen beendet wird, erscheint eine Liste entdeckter Bedrohungen auf dem Bildschirm und es wird Ihnen angeboten, [Aktionen](#) zur ihrer Neutralisierung zu wählen.



Abbildungen 7 und 8. Scanner und Fenster zur Auswahl der Scan-Objekte

Verdächtige Dateien dem Virenlabor von Doctor Web zusenden

Bei Bedarf können Sie verdächtige ZIP-Archive (eventuell Dateien mit JAR- und APK-Erweiterung), in denen Sie schädliche Programme vermuten, oder vertrauenswürdige ZIP-Archive, bei denen es sich um vermutliche Fehlalarme handelt, an das **Doctor Web** Virenlabor senden:

1. Wählen Sie die Datei in der Liste des Dateiverwaltungssystems aus (s. [Abbildung 8](#)), tippen Sie danach auf **Dem Virenlabor zusenden**.
2. Geben Sie im nächsten Fenster Ihre e-Mail-Adresse ein, wenn Sie die Ergebnisse der Analyse der zugesandten Datei erhalten möchten.
3. Wählen Sie eine der Kategorien für Ihre Anfrage aus:
 - **Verdacht auf Infizierung**, wenn Sie glauben, dass die Datei eine Bedrohung darstellt;
 - **Fehlalarm** oder **Fehlalarm der Origins Tracing**, wenn Sie glauben, dass die Datei fehlerhaft Bedrohungen zugeordnet wurde.

Die Auswahl einer der angebotenen Kategorien im Falle des Fehlalarms erfolgt aufgrund des Namens der vermutlich in der zugesandten Datei enthaltenen Bedrohung: Enthält der Name das Suffix ".origin", so sollte die Kategorie **Fehlalarm der Origins Tracing** und in anderen Fällen - die Kategorie **Fehlalarm** gewählt werden.

4. Tippen Sie auf **Senden**.



Sie können ZIP-Archive bis zu 10 MB an das **Doctor Web** Virenlabor senden.

Scanner konfigurieren

Um den Scanner einzustellen, rufen Sie im Hauptbildschirm das App-Menü auf, wählen Sie den Menüpunkt **Einstellungen** aus und navigieren Sie anschließend zu **Scanner**. Hier stehen Ihnen die folgenden Einstellungen zur Verfügung:

- Um die Prüfung von Dateien in Archiven zu aktivieren, setzen Sie ein Häkchen bei **Dateien in Archiven im Bereich Scanner**.



Standardmäßig ist die Archivprüfung deaktiviert. Durch die Aktivierung der Archivprüfung kann die Operationsgeschwindigkeit des Betriebssystems beschränkt und die Batterielaufzeit reduziert werden. Dabei beeinflusst die Deaktivierung der Archivprüfung den Schutzstatus nicht, da die Installationsdateien für Android-Betriebssysteme (.apk) durch den Dateiwatcher überprüft werden, unabhängig davon, welcher Wert für diesen Parameter festgelegt wurde.

- Um während des Scan-Vorgangs die Pfade der zu überprüfenden Dateien für jeden Kern der Geräte mit Mehrkernprozessoren einzeln anzeigen zu lassen, setzen Sie das Häkchen bei **Anzeige nach Kern** im Abschnitt **Scanner**.
- Um die Überprüfung des Systems auf Adware und PUAs (darunter auch Dialer und Scherzprogramme) zu aktivieren/deaktivieren, wählen Sie den Punkt **Optionen** im Bereich **Scanner** und setzen/wählen Sie das Häkchen bei **Adware** und **Riskware** ab.
- Um die SD-Karte auf Windows-Autostart-Dateien zu überprüfen, setzen Sie ein Häkchen bei **Autorun-Dateien** im Bereich **Allgemein**. Diese Einstellung wird auch bei Nutzung des Dateiwatchers verwendet.

Es ist empfehlenswert, das Dateisystem regelmäßig zu scannen, z. B. wenn der Wächter einige Zeit nicht aktiv war. In der Regel reicht dabei eine schnelle Systemprüfung aus.

Statistik

Die App protokolliert Ereignisse, die mit dem Betrieb des Scanners (darunter Informationen über den Modus und Ergebnisse des Scans sowie erkannte Sicherheitsbedrohungen) verbunden sind. Aktionen der App, insbesondere des Scanners, werden im Bereich **Aktionen** auf der Registerkarte **Statistik** nach Datum sortiert angezeigt.

Neutralisierung der Bedrohungen

Liste mit Bedrohungen einsehen

Wenn der **Dateiwatcher SpIDer Guard** eine Sicherheitsbedrohung erkennt, erscheint in der



Statusleiste des Geräts das Warnsymbol (für Android 5.0 und höher - ). Auf dem Bildschirm wird darüber hinaus eine Push-Benachrichtigung mit Informationen zu den erkannten Bedrohungen angezeigt. Tippen Sie in der **Benachrichtigungsleiste** auf die Benachrichtigung mit Informationen über die Anzahl entdeckter Bedrohungen, um die Liste mit allen erkannten schädlichen Objekten zu öffnen.



Unter Android 5.0 und höher wird die Benachrichtigung in der **Benachrichtigungsleiste** solange über alle laufenden Anwendungen eingeblendet, bis Sie eine Aktion für die Bedrohung durchführen oder die Benachrichtigung mit dem Finger wegswischen. Unter Android 5.0 und höher werden Benachrichtigungen über erkannte Bedrohungen ebenfalls auf dem Sperrbildschirm angezeigt. Vom Sperrbildschirm können Sie dann direkt die Liste erkannter Bedrohungen aufrufen.



Bei der Überprüfung Ihres Geräts durch den [Scanner](#) öffnet sich die Liste mit den entdeckten Bedrohungen automatisch, nachdem der Scanvorgang beendet wurde. Die Liste erkannter Bedrohungen kann erst dann geschlossen werden, nachdem für jede Bedrohung eine Aktion gewählt wurde.

Folgende Informationen werden für jede Bedrohung angezeigt:

- Bedrohungsname;
- Pfad der Datei, die eine Bedrohung enthält.

Für gefundene Bedrohungen, die nicht als Viren eingestuft werden, wird in Klammern der entsprechende Bedrohungstyp angezeigt: Adware, Riskware, Scherzprogramm oder Hacktool.

Aktionen für Bedrohungen verwenden

Tippen Sie in der Liste auf die Bedrohung, um alle möglichen Aktionen anzuzeigen und eine davon auszuführen. Nutzer von **Dr.Web** können eine der folgenden vier Aktionen auswählen:

- **Löschen** – die Bedrohung wird komplett aus dem Speicher des Geräts gelöscht
- **In Quarantäne** – die Bedrohung wird in einen speziellen Ordner verschoben und vom System isoliert



Wenn eine Bedrohung in der installierten Anwendung entdeckt wurde, wird es unmöglich sein, sie in die Quarantäne zu verschieben. In diesem Fall fehlt die Aktion **In Quarantäne** in der Liste.

- **Überspringen** – die Anwendung überspringt die Bedrohung und führt keine Aktion dafür aus
- **Fehlalarm melden** – Es wird Ihnen angeboten, das bedrohliche Objekt dem **Virenlabor von Doctor Web** zusammen mit der Meldung darüber, dass dieses Objekt keine Bedrohung darstellt und fälschlicherweise von dem Antivirusprogramm als verdächtig eingeschätzt wurde, zuzusenden. Um die Ergebnisse der Dateianalyse zu erhalten, geben Sie Ihre E-Mail-Adresse in dem entsprechenden Eingabefeld an und tippen Sie auf **Senden**.



Die Aktion **Fehlalarm melden** ist nur für modifizierte Bedrohungen möglich, die das Suffix „origin“ enthalten und im Systembereich gefunden wurden.

Sie können akustische Benachrichtigungen für Entdecken, Löschen und Verschieben von Bedrohungen in Quarantäne einstellen. Dafür rufen Sie auf dem Hauptbildschirm des Programms das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**. Danach setzen Sie ein Häkchen bei **Ton** im Bereich **Allgemein** im Einstellungsbildschirm (s. [Abbildung 6](#)).

Bedrohungen bei Systemanwendungen entdecken

In manchen Fällen können die Systemanwendungen, die von Herstellern auf Ihr Gerät vorinstalliert werden, Malware-spezifische Funktionen ausführen. Somit kann **Dr.Web** diese Anwendungen beim Scannen als Sicherheitsbedrohungen beurteilen und eine entsprechende Warnung anzeigen. Die standardmäßigen Aktionen zur [Neutralisierung von Bedrohungen](#) können dabei nicht eingesetzt werden. Sie können aber wie folgt vorgehen:

- Beenden Sie die Anwendung über die Einstellungen des Geräts (tippen Sie in der Liste installierter Anwendungen auf dem Bildschirm **Einstellungen** -> **Apps** auf den Namen der Anwendung, die als Bedrohung erkannt wurde. Tippen Sie auf dem Bildschirm mit Informationen zur App auf **Beenden erzwingen**).



Diesen Vorgang müssen Sie bei jedem Neustart Ihres Geräts wiederholen.



- Beenden Sie die Anwendung über die Einstellungen des Geräts (tippen Sie in der Liste installierter Anwendungen auf dem Bildschirm **Einstellungen** -> **Apps** auf den Namen der Anwendung, die als Bedrohung erkannt wurde. Tippen Sie auf dem Bildschirm mit Informationen zur App auf **Deaktivieren**).



Dieser Vorgang ist nur unter Android 4.0 oder höher möglich. Sie müssen diesen Vorgang nach jedem Neustart des Geräts nicht wiederholen.

- Wenn die Firmware auf Ihrem Gerät verändert wurde, können Sie es auf die Werkseinstellungen zurücksetzen und die Original-Software des Herstellers nutzen.
- Wenn Sie die Original-Software des Herstellers des mobilen Geräts nutzen, wenden Sie sich für nähere Informationen über die App an den Hersteller Ihres Geräts.
- Auf einem Gerät mit dem root-Zugriff können Sie versuchen, die Anwendung mit Hilfe spezieller Tools zu entfernen.

Des Weiteren können Sie die Benachrichtigungen über Bedrohungen, die in bekannten Systemanwendungen erkannt werden, mit Hilfe der Option **System-Anwendungen** im Bereich **Allgemeine Einstellungen** -> **Erweitert** im Einstellungsbildschirm deaktivieren (s. Abbildung 6).

Sperr-Software bearbeiten

Mit **Dr.Web** schützen Sie Ihr mobiles Gerät vor weit verbreiteten Ransomware für Android-Plattformen. Diese Art von Software ist sehr gefährlich. Damit können die auf Smartphones und Tablet-PCs als Wechseldatenträgern gespeicherten Dateien verschlüsselt werden. Der Bildschirm des mobilen Geräts kann gesperrt werden, wobei eine Nachricht mit einer Lösegeld-Forderung für Freigabe von Dateien bzw. des Geräts angezeigt wird.

Die Erpresser-Software gefährdet Fotos, Videos und Dokumente, die auf der Wechselkarte eines mobilen Geräts gespeichert werden. Darüber hinaus raubt die Ransomware unterschiedliche Informationen zu dem infizierten Gerät (darunter auch IMEI), die Daten aus dem Adressbuch (Kontaktnamen, Rufnummern und E-Mail-Adressen) und übermittelt diese an die Server der böswilligen Benutzer. Die ein- und ausgehenden Anrufe werden durch die Ransomware nachverfolgt und können dadurch gesperrt werden. Alle gesammelten Daten, darunter auch Daten über die Anrufe, werden auch an den Verwaltungsserver übermittelt.

Die erpresserische Schadsoftware wird durch **Dr.Web** erkannt und entfernt, soweit diese versucht, ins geschützte Gerät einzudringen. Die Ransomware wächst aber ständig in Anzahl und Vielfalt. Wenn die **Dr.Web Virendatenbanken** eine gewisse Zeit lang nicht aktualisiert wurden und keine Informationen zu neuen Typen enthalten, kann es vorkommen, dass die Sperrsoftware auf dem Gerät installiert wird.

Wenn das mobile Endgerät mit dem aktivierten Dateiwatcher **SpIDer Guard** durch die Ransomware gesperrt wurde, können Sie wie folgt vorgehen, um das Gerät freizugeben:

1. Schließen Sie Ihr mobiles Endgerät für 5 Sekunden an eine Stromquelle an.
2. Stecken Sie innerhalb von den nächsten 10 Sekunden einen Kopfhörer ein.
3. Stecken Sie innerhalb der nächsten 5 Sekunden den Kopfhörer aus.
4. Schütteln Sie innerhalb der nächsten 10 Sekunden kräftig Ihr mobiles Endgerät.



5. **Dr.Web** beendet alle aktiven Prozesse auf dem Gerät, darunter auch den Prozess, der durch die Ransomware gestartet wurde. Danach ertönt ein kurzes Vibrationssignal (vorausgesetzt, dass diese Funktion auf dem Gerät vorhanden ist). Es öffnet sich der Bildschirm von **Dr.Web**.



Bitte beachten Sie, dass die Daten anderer Anwendungen beim Beenden der aktiven Prozesse verloren gehen können, wenn diese Anwendungen bei Sperrung des Geräts aktiv waren.

6. Es wird empfohlen, die **Dr.Web Virendatenbanken** nach Freigabe des Geräts zu aktualisieren und einen schnellen Scan des Systems durchzuführen bzw. die böswillige Anwendung zu entfernen.

Anruf- und SMS-Filter

Dr.Web ermöglicht das Filtern von SMS-Nachrichten und Anrufen, indem unerwünschte Nachrichten und Anrufe, z.B. Werbung, sowie Anrufe und Nachrichten von unbekannten Nummern gesperrt werden können.



Für Android 4.4 kann das korrekte Filtern von SMS-Nachrichten nicht gewährleistet werden.

Auf mobilen Dual-SIM-Geräten kann der Anruf- und SMS-Filter eventuell nicht ordnungsgemäß funktionieren.

Die App bietet Ihnen die Möglichkeit, einen Filter für Anrufe und Kurznachrichten auszuwählen. Außer voreingestellten Profilen, mit denen die Filtermodi festgelegt werden, können auch benutzerdefinierte Profile erstellt werden. Für jedes dieser Profile können eigene Filtereinstellungen festgelegt werden.



Im Zentralschutz-Modus können die Einstellungen des Anruf- und SMS-Filters entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein.

Informationen zu gesperrten Anrufen und Nachrichten sind im Bereich **Gesperrte Anrufe und SMS** verfügbar.

Filtermodus wählen

Filtern von Anrufen und Nachrichten erfolgt in einem der folgenden Modi:

- **Alles durchlassen.** In diesem Modus ist Filterung deaktiviert, d.h. alle eingehenden Anrufe und SMS-Nachrichten werden durchgelassen.
- **Alles sperren.** Dabei werden alle eingehenden Anrufe und SMS-Nachrichten gesperrt.
- **Telefonbuch.** In diesem Modus werden eingehende Anrufe und SMS-Nachrichten nur von den ins Telefonbuch eingetragenen Nummern durchgelassen.
- **Blacklist.** In diesem Filtermodus werden Anrufe und SMS-Nachrichten von den in der Blacklist eingetragenen Nummern gesperrt.

Dieser Filtermodus wird durch das einstellbare Profil festgelegt. **Dr.Web** erlaubt es, eine uneingeschränkte Anzahl von Profilen zu erstellen. Für jedes dieser Profile kann eine Liste der Rufnummern erstellt sowie Aktionen (durchlassen/sperrn) für Anrufe und Nachrichten von den Nummern auf dieser Liste festgelegt werden.



Im benutzerdefinierten Filtermodus werden Kontakte auf der Blacklist zusätzlich gesperrt.

Blacklist

Der Blacklist können Nummern, von denen Sie eingehende Anrufe und Nachrichten Sie sperren möchten, hinzugefügt werden. Dabei werden die Anrufe und Nachrichten von den Nummern auf der Blacklist sowie im Filtermodus **Blacklist** als auch bei der Auswahl eines beliebigen benutzerdefinierten Profils zusätzlich zu den Nummern, die auf der Liste dieses Profils sind, gesperrt. Somit wird das Filtern aufgrund der Blacklist nur im Filtermodus **Alles durchlassen** deaktiviert.

Blacklist erstellen

1. Um eine Blacklist einzurichten, tippen Sie auf dem Hauptbildschirm der App auf den Filterbereich. Tippen Sie dann im angezeigten Menü zur Auswahl eines Profils auf **Einstellungen**.
2. Wechseln Sie zu **Blacklist**.
3. Tippen Sie auf **Hinzufügen**, um eine Blacklist zu erstellen. Sie können Kontakte und Rufnummern wie folgt auswählen:
 - aus der Kontaktliste;
 - aus dem Anruf- und Nachrichtenlog;
 - manuell durch Eingabe von Rufnummern und Informationen dazu.

Zur Suche von Kontakten im Telefonbuch sowie in den Anruf- und Nachrichtenlogs können Sie die Suchfunktion nutzen. Tippen Sie dafür auf **Suche**. Sie können jeweils eine bzw. mehrere Rufnummern fürs Hinzufügen zur Blacklist wählen.

Um ausgewählte Nummern zur Liste hinzuzufügen, tippen Sie auf **Hinzufügen**.

4. Für jeden Kontakt auf der Blacklist können Sie eine der folgenden Aktionen wählen:
 - **Anrufe und SMS sperren** – um alle eingehenden Anrufe und Nachrichten von diesem Kontakt zu sperren.
 - **Nur Anrufe sperren** – um nur eingehende Anrufe von einem bestimmten Kontakt zu sperren. Die Nachrichten werden dabei durchgelassen.
 - **Nur SMS sperren** – um nur Nachrichten von einem bestimmten Kontakt eingehen, zu sperren. Die Anrufe werden dabei durchgelassen.

Standardmäßig wird die Aktion **Anrufe und SMS sperren** für jeden hinzugefügten Kontakt festgelegt. Gegebenenfalls können Sie diese Einstellung ändern.

5. Um Angaben eines Kontakts auf der Blacklist zu ändern, tippen Sie darauf und halten Sie den Kontakt gedrückt bzw. streichen Sie den Kontakt nach links oder rechts. Im geöffneten Menü tippen Sie auf **Editieren**. Bearbeiten Sie die Felder **Name** und **Nummer**. Tippen Sie auf **Speichern**.



Angaben der Kontakte aus dem Telefonbuch sowie unterdrückter Rufnummern können nicht bearbeitet werden.

6. Um eine Nummer aus der Blacklist zu entfernen, tippen Sie darauf und halten Sie die Nummer gedrückt bzw. streichen Sie sie nach rechts oder links. Im geöffneten Menü tippen Sie auf **Löschen**.
7. Sie können auch eine Liste der Schlagwörter erstellen, damit alle SMS-Nachrichten, die solche Schlagwörter enthalten, gesperrt werden. Dafür wählen Sie die Option **Schlagwort** im Menü, das Optionen fürs Hinzufügen der Kontakte zur Blacklist bietet. Im Bereich **SMS Sperrung nach Schlagwörtern** geben Sie ein Schlagwort ein und tippen Sie auf **Hinzufügen**.



Blacklist bereinigen

Um alle Kontakte aus der Blacklist zu entfernen, tippen Sie auf das Menü-Symbol und wählen Sie **Liste leeren**. Bestätigen Sie im entsprechenden Fenster den Löschvorgang.

Filterprofil erstellen

Dr.Web ermöglicht die Erstellung benutzerdefinierter Filtermodi für Anrufe und Nachrichten.

Neues Profil erstellen

1. Tippen Sie in der Liste verfügbarer Profile auf **Einstellen**.
2. Im Tab **Profile** tippen Sie auf **Profil hinzufügen**.
3. Geben Sie den Profilnamen ein.
4. Wählen Sie eine Aktion für eingehende Anrufe und Nachrichten von den Nummern, die auf der Liste in diesem Profil sind. Folgende Aktionen sind verfügbar:
 - **Nur Kontakte aus der Liste erlauben** – damit Anrufe und Nachrichten nur von den Nummern, die auf der Liste in diesem Profil sind, durchgelassen werden
 - **Kontakte aus der Liste sperren** – damit Anrufe und Nachrichten von den Nummern, die auf der Liste in diesem Profil sind, gesperrt werden
5. Tippen Sie auf **Kontakt hinzufügen**, um eine Kontaktliste zu erstellen. Sie können die Nummern wie folgt auswählen:
 - aus der Kontaktliste
 - aus dem Anruf- und Nachrichtenlog
 - manuell durch Eingabe der Rufnummern und Informationen dazu

Zur Suche von Kontakten im Telefonbuch sowie in den Anruf- und Nachrichtenlogs können Sie die Suchfunktion nutzen. Tippen Sie dafür auf **Suche**. Sie können jeweils eine bzw. mehrere Rufnummern fürs Hinzufügen zur Profilliste wählen.

Um ausgewählte Nummern zur Liste hinzuzufügen, tippen Sie auf **Hinzufügen**. Die Anzahl der Kontakte auf der Profilliste wird neben dem Profilnamen rechts in Klammern angezeigt.



Die Kontaktliste des Profils kann nicht leer sein.

6. Um Angaben eines Kontakts auf der Liste zu ändern, tippen Sie darauf und halten Sie den Kontakt gedrückt bzw. streichen Sie den Kontakt nach rechts oder links. Im geöffneten Menü tippen Sie auf **Editieren**. Bearbeiten Sie die Felder **Name** und **Nummer**. Tippen Sie auf **Speichern**.



Die Angaben der Kontakte aus dem Telefonbuch sowie der privaten Nummern können nicht bearbeitet werden.

7. Um einen Kontakt aus der Profilliste zu entfernen, tippen Sie darauf und halten Sie den Kontakt gedrückt bzw. streichen Sie nach rechts oder links. Im geöffneten Menü tippen Sie auf **Löschen**.



Die aus einem benutzerdefinierten Profil gelöschten Kontakte bleiben in der Kontaktliste des Telefonbuches erhalten.



Gesperrte Anrufe und Nachrichten einsehen

Im Anruf- und SMS-Filter auf dem Hauptbildschirm der App wird die Anzahl gesperrter Anrufe und SMS-Nachrichten angezeigt. Um die Listen gesperrter Anrufe und Nachrichten einzusehen, tippen Sie auf das entsprechende Symbol:

-  – um gesperrte Anrufe einzusehen
-  – um gesperrte Nachrichten einzusehen

Neben den Listennamen rechts wird die Anzahl der nicht eingesehenen Anrufe/Nachrichten in Klammern angezeigt. Für jeden Anruf/jede Nachricht auf der Liste werden folgende Informationen angezeigt:

- Datum und Uhrzeit des eingehenden Anrufs/der eingehenden Nachricht
- Rufnummer und Name des Anrufers/SMS-Absenders

Aktionen für gesperrte Anrufe/Nachrichten

1. Sie können den Anrufer, dessen Anruf gesperrt wurde, zurückrufen. Dafür tippen Sie auf den Anruf in der Liste. Es öffnet sich der Bildschirm mit gewählter Rufnummer. Um einen Anruf zu tätigen, tippen Sie auf **Anrufen**.
2. Beim Tippen auf eine Nachricht auf der Liste gesperrter Nachrichten öffnet sich der Text sowie die Angaben der Nachricht. Es wird Ihnen angeboten, eine der folgenden Aktionen dafür zu wählen:
 - **Wiederherstellen** – damit die Nachricht in die Liste eingehender Nachrichten verschoben wird



Der Punkt **Wiederherstellen** ist nicht verfügbar für mobile Endgeräte unter Android ab Version 4.4.

- **Löschen** – damit die Nachricht gelöscht wird

Aktualisierung

Zur Entdeckung von Sicherheitsbedrohungen verwendet **Dr.Web** spezielle **Virendatenbanken von Dr.Web**, die Spezialisten von **Doctor Web** mehrmals täglich mit Informationen über alle neuen Sicherheitsrisiken, denen Android-Geräte ausgesetzt sein können, aktualisieren. Die Datenbanken bedürfen einer regelmäßigen Aktualisierung, da immer neue Schadprogramme erscheinen. Dafür können die Virendatenbanken über Internet aktualisiert werden.

Auf dem Hauptbildschirm der App unter **Update** wird das Datum der letzten Aktualisierung angezeigt.



Im **Zentralschutz-Modus** ist das manuelle Update nicht möglich. Updates werden vom Zentralschutz-Server automatisch heruntergeladen. Wenn der Zentralschutz-Server den mobilen Modus zulässt, können Sie beim Abbruch der Verbindung mit dem Zentralschutz-Server Virendatenbanken manuell aktualisieren.

Aktualisierung

1. Um die Virendatenbanken zu aktualisieren, tippen Sie auf dem Hauptbildschirm der App auf den Abschnitt mit Informationen zu Updates.
2. Die Aktualisierung wird automatisch gestartet.



Sobald die App installiert ist, sollten Sie die Virendatenbanken aktualisieren, damit **Dr.Web** die aktuellsten Informationen zu bekannten Bedrohungen verwendet kann. Die Virensignaturen, Informationen zu deren Merkmalen und Verhaltensmustern werden sofort aktualisiert, sobald neue Bedrohungen durch Spezialisten des **Virenlabors von Doctor Web** entdeckt werden. Manchmal geschieht dies mehrmals pro Stunde.

Aktualisierungseinstellungen

Standardmäßig werden die Updates automatisch vier Mal am Tag geladen. In dem Bereich **Update** im Einstellungsbildschirm (s. [Abbildung 6](#)) können Sie die Verwendung von mobilen Netzwerken beim Herunterladen von Updates erlauben/verbieten. Damit keine mobilen Netzwerke beim Herunterladen von Updates benutzt werden, setzen Sie ein Häkchen bei **Mobiles Internet nicht benutzen**. Wenn keine aktiven Netzwerke entdeckt werden, wird es Ihnen angeboten, 3G- bzw. GPRS-Netze zu nutzen. Eventuelle Änderungen dieser Einstellung haben keine Auswirkungen auf andere Anwendungen Ihres mobilen Geräts.



Bei der Aktualisierung werden die Daten übers Netzwerk geladen. Für die Datenübertragung können zusätzliche Kosten anfallen. Mehr dazu erfahren Sie bei Ihrem Mobilfunkanbieter.

[Im Zentralschutz-Modus](#) können die Einstellungen des Scanners entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein.

Quarantäne

Entdeckte Bedrohungen werden durch **Dr.Web** in Quarantäne – in einen speziellen Ordner, der zur deren Isolierung und sicheren Speicherung dient – verschoben.

Bedrohungen in Quarantäne behandeln

1. Zum Einsehen einer Liste der in die Quarantäne verschobenen Bedrohungen auf dem Hauptbildschirm des Programms wählen Sie den Punkt **Quarantäne**.
2. Es öffnet sich die Liste aller Bedrohungen, die sich in der Quarantäne befinden (s. [Abbildung 9](#)).
3. Tippen Sie auf eine Bedrohung in der Liste, um folgende Informationen dazu einzusehen:
 - Dateiname
 - Pfad der Datei
 - Datum der Verschiebung in die Quarantäne

Darüber hinaus können Sie dem Link im Bereich **Informationen im Internet** folgen, um weitere Informationen zu ähnlichen Bedrohungen im Internet auf der Webseite von **Doctor Web** einzusehen.

4. Sie können eine der folgenden Aktionen für jede Bedrohung ausführen:
 - **Wiederherstellen** – um die Datei in den Ordner, in dem sich diese Datei vor ihrer Verschiebung befand, zu bringen (verwenden Sie diese Funktion nur in dem Fall, wenn kein Zweifel besteht, dass die Datei sicher ist).
 - **Löschen** – um die Datei aus der Quarantäne und aus dem System zu löschen.

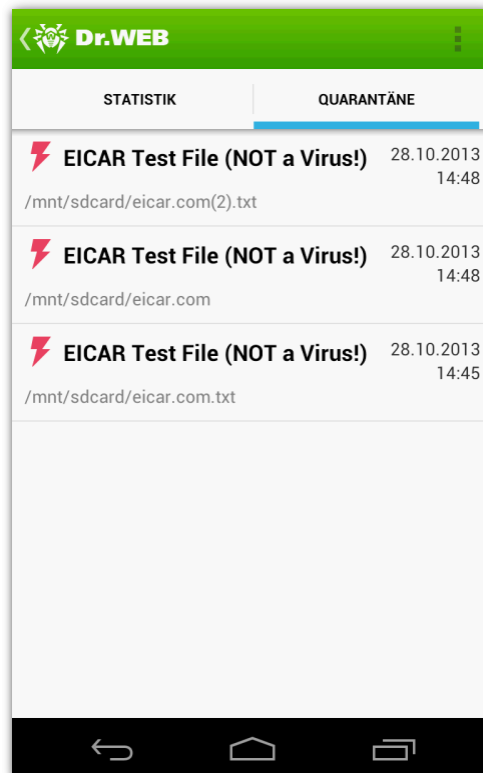


Abbildung 9. Quarantäne

Größe von Quarantäne

Sie können Informationen zum Speicherplatz, der durch Quarantäne eingenommen wird, sowie zum freien Speicherplatz auf der SD-Karte einsehen. Dafür rufen Sie das Anwendungsmenü im Tab **Quarantäne** auf und wählen den Punkt **Quarantäne-Größe** aus.

Statistik

Dr.Web zeichnet Informationen über erkannte Bedrohungen und Aktionen der App auf. Um Statistiken zur App-Nutzung anzusehen, öffnen Sie auf dem Hauptbildschirm das Menü der App und wählen Sie den Punkt **Statistik** aus.

Im **Statistik**-Tab finden Sie zwei Informationsbereiche (s. [Abbildung 10](#)):

- **Insgesamt**-Bereich, der Informationen zur Gesamtzahl überprüfter Dateien, entdeckter und neutralisierter Bedrohungen beinhaltet.
- **Aktionen**-Bereich, der Informationen zu Prüfungsbeginn/-ende, Aktivierung/Deaktivierung des Wächters sowie zu entdeckten Bedrohungen und Aktionen zu deren Neutralisierung beinhaltet. Tippen Sie auf den Namen einer Bedrohung, um ihre Beschreibung auf der Webseite von **Doctor Web** abzurufen.

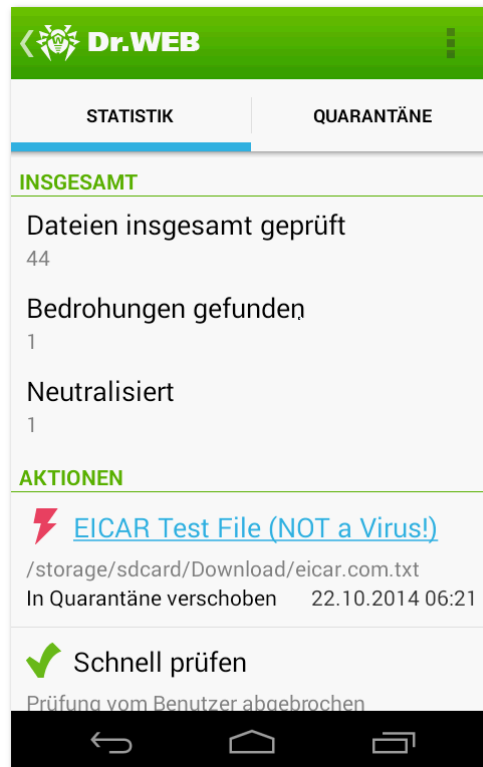


Abbildung 10. Statistik

Statistik bereinigen

Um alle erfassten Statistiken zur App zu löschen, rufen Sie das Menü der App auf und wählen Sie den Punkt **Statistik bereinigen** aus.

Ereignislog

Die App zeichnet alle Ereignisse in einem Protokoll auf, das auf der SD-Karte gespeichert und bei Bedarf an den technischen Support von **Doctor Web** gesendet wird, falls die App nicht ordnungsgemäß funktioniert.

Um das Ereignislog zu speichern:

1. Tippen Sie auf das **Menü** im **Statistik**-Tab und wählen Sie den Punkt **Protokoll speichern** aus.
2. Das Log wird in der Datei DrWeb_Log.txt gespeichert. Diese Datei befindet sich im Verzeichnis Android/data/com.drweb/files auf der SD-Karte.

Dr.Web Diebstahlschutz

Der **Dr.Web Diebstahlschutz** hilft Ihnen, Ihr Telefon beim Verlust oder Diebstahl zu orten bzw. seine Funktionen sofort zu sperren.



Im Zentralschutz-Modus können die Einstellungen des **Dr.Web Diebstahlschutzes** entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein.

Der **Dr.Web Diebstahlschutz** wird mit speziellen SMS-Befehlen verwaltet. Für den Zugriff auf die Einstellungen vom **Dr.Web Diebstahlschutz** ist ein spezielles Passwort einzugeben, das bei der



Ersteinstellung festgelegt wird. Dieses Passwort müssen Sie sich merken, da alle Funktionen vom **Dr.Web Diebstahlschutz** damit gesteuert werden. Sie werden es außerdem fürs Entsperren Ihres Gerätes brauchen, falls es gesperrt wird. Wenn Sie das für den **Dr.Web Diebstahlschutz** festgelegte Passwort vergessen haben, können Sie den speziellen Service zur Zurücksetzung des Passworts und Freigabe Ihres Gerätes nutzen.

Darüber hinaus können Sie mit dem **Dr.Web Diebstahlschutz** eine Freundesliste (bis zu 5 Telefonnummern) erstellen. Von den Telefonnummern ihrer Freunde aus wird es möglich sein, SMS-Befehle auch dann zu senden, wenn Sie Ihr Passwort für den **Dr.Web Diebstahlschutz** vergessen haben.



Auf mobilen Dual-SIM-Geräten kann die Komponente **Dr.Web Diebstahlschutz** nicht ordnungsgemäß funktionieren.

Wenn der **Dr.Web Diebstahlschutz** aktiviert ist, sind einige Bereiche der App (**Einstellungen zurücksetzen**, **Sicherungskopie** und **Modus**) passwortgeschützt. Um ihre Einstellungen ändern zu können, müssen Sie das Passwort des **Dr.Web Diebstahlschutzes** angeben.

Ersteinstellung

Beim ersten Start vom **Dr.Web Diebstahlschutz** öffnet sich das Fenster mit dem Einstellungsassistenten, mit dem Sie die Grundfunktionen einstellen können:

- Tippen Sie auf **Weiter**, um zur Einstellung der Grundfunktionen vom **Dr.Web Diebstahlschutz** zu wechseln.
- Tippen Sie auf **Abbrechen**, wenn Sie den **Dr.Web Diebstahlschutz** später konfigurieren wollen.

Ersteinstellung des Dr.Web Diebstahlschutzes mit dem Einstellungsassistenten

1. Im ersten Einstellungsschritt vom **Dr.Web Diebstahlschutz** legen Sie ein Passwort fest (das Passwort muss mindestens 4 Zeichen enthalten). Dieses Passwort dient zur Steuerung aller Funktionen vom **Dr.Web Diebstahlschutz**. Gegebenenfalls aktivieren Sie die Option Zeichen bei Passworteingabe anzeigen. Tippen Sie dafür auf das Symbol  rechts neben dem Eingabefeld. Um das Passwort auszublenden, tippen Sie auf das Symbol . Tippen Sie auf **Weiter**.
2. Bestätigen Sie das eingegebene Passwort. Tippen Sie auf **OK**.
3. Konfigurieren Sie die Freundesliste. Tippen Sie auf **Weiter**.



Auf Geräten unter Android 4.4 und höher muss die Freundesliste mindestens eine Telefonnummer enthalten.

4. Wenn Sie bisher kein Google-Konto angelegt haben, öffnet sich im weiteren Verlauf ein Eingabefeld zur Angabe Ihrer E-Mail-Adresse, um den **Dr.Web Diebstahlschutz** auf dem Server von **Doctor Web** zu registrieren. Dies ist notwendig, um Ihnen bei Bedarf den Code zur Entsperrung des Geräts bzw. zur Eingabe eines neuen Passworts zuzusenden, wenn Sie das für den **Dr.Web Diebstahlschutz** festgelegte Passwort vergessen haben. Geben Sie eine gültige E-Mail-Adresse an und tippen Sie auf **Weiter**.



Um Ihre E-Mail-Adresse auf dem Server zu registrieren, benötigen Sie eine aktive Internetverbindung.

5. Geben Sie einen Text ein, der auf dem Bildschirm Ihres Telefons im Fall seiner Sperrung angezeigt wird. Tippen Sie auf **Weiter**.
6. Die erstmalige Einstellung vom **Dr.Web Diebstahlschutz** ist damit abgeschlossen. Es wird Ihnen

angeboten, die bei der Anmeldung Ihres Google-Kontos angegebene E-Mail-Adresse (bzw. die im vorhergehenden Einstellungsschritt angegebene E-Mail-Adresse) auf dem Server von **Doctor Web** zu registrieren. Tippen Sie auf **Fertig**, um die Registrierung zu starten:

- bei einer erfolgreichen Registrierung wird der Einstellungsassistent geschlossen und der Einstellungsbildschirm vom **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) geöffnet;
- sollten bei der Registrierung Probleme auftreten, erscheint auf dem Bildschirm die Meldung mit der Fehlerbeschreibung. Es erfolgt keine Aktivierung vom **Dr.Web Diebstahlschutz** auf Ihrem Gerät.

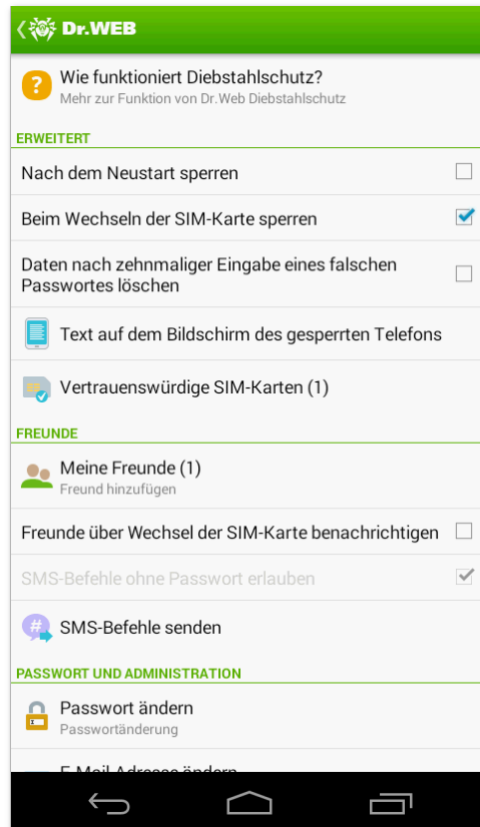


Abbildung 11. Einstellungen von Dr.Web Diebstahlschutz



Beim Wechseln zu den Einstellungen von **Dr.Web Diebstahlschutz** kann eine Meldung angezeigt werden, in der Sie aufgefordert werden, **Dr.Web** als Administrator des Geräts festzulegen. Sie haben diese Anforderung zu akzeptieren, damit **Dr.Web Diebstahlschutz** vollwertig funktionieren kann.

Hilfe aufrufen

Um Hilfe für den **Dr.Web Diebstahlschutz** aufzurufen, wählen Sie den Punkt **Wie funktioniert Diebstahlschutz?** im **Hilfe**-Bereich auf dem Einstellungsbildschirm von **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)).

Passwort ändern

Um das für den **Dr.Web Diebstahlschutz** festgelegte Passwort zu ändern, gehen Sie im Einstellungsbildschirm vom **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) wie folgt vor:

1. Tippen Sie im Abschnitt **Passwort und Administration** auf **Passwort ändern**.
2. Geben Sie das aktuelle Passwort ein. Tippen Sie auf **OK**.
3. Geben Sie ein neues Passwort ein. Tippen Sie auf **Weiter**.
4. Bestätigen Sie das neue Passwort. Tippen Sie auf **OK**.



Neue E-Mail-Adresse registrieren

Um die für den **Dr.Web Diebstahlschutz** auf dem Server von **Doctor Web** registrierte E-Mail-Adresse zu ändern, wählen Sie im Einstellungsbildschirm vom **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) die folgenden Aktionen:

1. Tippen Sie im Abschnitt **Passwort und Administration** auf **E-Mail-Adresse ändern**.
2. Geben Sie die E-Mail-Adresse für die Registrierung auf dem Server von **Doctor Web** ein. Tippen Sie auf **OK**.
3. Eine E-Mail mit der Bestätigung der durchgeführten Änderungen wird an die erstangemeldete E-Mail-Adresse geschickt.

Deaktivierung des Dr.Web Diebstahlschutzes

Um den **Dr.Web Diebstahlschutz** auf Ihrem Gerät zu deaktivieren, wählen Sie im Einstellungsbildschirm vom **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) die folgenden Aktionen:

1. Tippen Sie im Abschnitt **Passwort und Administration** auf **Dr.Web Diebstahlschutz deaktivieren**.
2. Geben Sie das für den **Dr.Web Diebstahlschutz** festgelegte Passwort ein und tippen Sie auf **Dr.Web Diebstahlschutz deaktivieren**.



Bei Deaktivierung vom **Dr.Web Diebstahlschutz** wird das Sicherheitsniveau wesentlich verringert!

Erweiterte Optionen einstellen

Um den **Dr.Web Diebstahlschutz** zu konfigurieren, wählen Sie den **Diebstahlschutz**-Bereich auf dem Hauptbildschirm der Anwendung aus. Für den Zugang zum Bildschirm mit den Einstellungen für den **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) müssen Sie das für den **Dr.Web Diebstahlschutz** beim ersten Start festgelegte Passwort eingeben. Wenn Sie das Passwort vergessen haben, senden Sie den SMS-Befehl **#RESETPASSWORD#** von einer Rufnummer, die auf Ihrer Freundesliste ist, an Ihr Gerät bzw. nutzen Sie den speziellen [Service](#).

Erweiterte Optionen

Um den **Dr.Web Diebstahlschutz** zu konfigurieren, gehen Sie im Bereich **Erweitert** auf dem Einstellungsbildschirm vom **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) wie folgt vor:

- Um das Telefon im Falle seines Neustarts zu sperren, aktivieren Sie die Option **Nach dem Neustart sperren**.
- Damit Ihr Telefon bei SIM-Kartenwechsel gesperrt wird, aktivieren Sie die Option **Beim Wechseln der SIM-Karte sperren**.
- Damit Ihre persönlichen Daten auf der SD-Karte nach 10-maliger falscher Passworteingabe vollständig gelöscht werden, aktivieren Sie die Option **Daten nach zehnmaliger Eingabe eines falschen Passwortes löschen**.
- Um den Text, der auf dem Bildschirm des gesperrten Telefons angezeigt wird, festzulegen, tippen Sie auf **Text auf dem Bildschirm des gesperrten Telefons** und geben Sie den Text ein (Sie können zum Beispiel Ihre Kontaktdaten angeben, damit man Ihnen das gefundene Telefon zurückgeben konnte). Tippen Sie dann auf **Speichern**.
- Um die Liste mit den vertrauenswürdigen SIM-Karten einzusehen und zu bearbeiten, tippen Sie auf **Vertrauenswürdige SIM-Karten**.



Vertrauenswürdige SIM-Karten

SIM-Karten, die in Ihrem mobilen Gerät genutzt werden, können der Liste vertrauenswürdiger SIM-Karten vom **Dr.Web Diebstahlschutz** hinzugefügt werden. Wird eine vertrauenswürdige SIM-Karte auf dieser Liste durch eine andere ersetzt, wird Ihr Gerät durch **Dr.Web Diebstahlschutz** nicht gesperrt. Neue SIM-Karten werden zur Liste beim Neustart des Geräts bzw. beim Start von **Dr.Web** hinzugefügt. Sie können auch den Betrieb ohne SIM-Karte zu dieser Liste hinzufügen.



Der Betrieb ohne SIM-Karte kann aktiviert werden, wenn keine SIM-Karte in Ihrem Gerät installiert ist und wenn Ihr Gerät den installierten Anwendungen keinen Zugriff auf Informationen über die SIM-Karte erlaubt. Dadurch können Sie eine Fehlermeldung über eine fehlende SIM-Karte erhalten. Wenn Sie einen solchen Betriebsmodus jedoch als vertrauenswürdig festlegen, werden alle Funktionen vom **Dr.Web Diebstahlschutz** in vollem Umfang für Sie zugänglich sein.

Tippen Sie zum Einsehen und Bearbeiten der Liste von vertrauenswürdigen SIM-Karten auf **Vertrauenswürdige SIM-Karten** im Bereich **Erweitert** vom **Dr.Web Diebstahlschutz**:

1. Standardsmäßig werden hinzugefügte SIM-Karten SIM1, SIM2 usw. genannt. Um einer SIM-Karte einen neuen Namen zu geben, tippen Sie auf deren Namen in der Liste (bzw. tippen Sie auf den Namen und halten Sie diesen gedrückt, im geöffneten Menü wählen Sie **Editieren** aus). Es öffnet sich ein Fenster mit Informationen zur SIM-Karte. Geben Sie hier einen neuen Namen im Feld **Vorname** ein und tippen Sie auf **Speichern**.
2. Um eine SIM-Karte aus der Liste vertrauenswürdiger SIM-Karten zu löschen, tippen und halten Sie ihren Namen gedrückt. Im geöffneten Menü wählen Sie **Löschen** aus.



Die in Ihrem Gerät aktuell genutzte SIM-Karte kann aus der Liste vertrauenswürdiger SIM-Karten nicht gelöscht werden.

Freundesliste

Der **Dr.Web Diebstahlschutz** ermöglicht das Hinzufügen von bis zu 5 Rufnummern zur Freundesliste. Für diese Rufnummern können Sie den Versand von SMS-Befehlen an Ihr Telefon ohne Passworteingabe einstellen. Darüber hinaus können Sie einen SMS-Befehl zur Deaktivierung vom **Dr.Web Diebstahlschutz** und Zurücksetzung des dafür festgelegten Passworts von diesen Rufnummern senden.



Auf Geräten unter Android 4.4 und höher muss die Freundesliste mindestens eine Telefonnummer enthalten.

Freundesliste konfigurieren

1. Auf dem Einstellungsbildschirm vom **Dr.Web Diebstahlschutz** (s. [Abbildung 11](#)) tippen Sie im **Freunde**-Bereich auf **Meine Freunde**.
2. Tippen Sie auf **Hinzufügen**, um eine Freundesliste zu erstellen. Sie können Kontakte und Rufnummern wie folgt auswählen:
 - aus der Kontaktliste;
 - aus dem Anruf- und Nachrichtenlog;
 - manuell durch Eingabe von Rufnummern und Informationen dazu

Zur Suche von Kontakten im Telefonbuch sowie in den Anruf- und Nachrichtenlogs können Sie die Suchfunktion nutzen. Tippen Sie dafür auf die **Suche**. Sie können jeweils eine bzw. mehrere Rufnummern zur Liste hinzufügen.



Um ausgewählte Nummern zur Liste hinzuzufügen, tippen Sie auf **Hinzufügen**.

3. Um Angaben eines Kontakts auf der Liste zu ändern, tippen Sie auf ihn und bearbeiten Sie die Werte in den Feldern **Name** und **Nummer**. Tippen Sie auf **Speichern**.
4. Um eine Nummer aus der Liste zu entfernen, tippen Sie auf diese Nummer und halten Sie sie gedrückt. Im geöffneten Menü tippen Sie auf **Löschen**.



Unter Android 4.4 können Sie zwar alle Kontakte aus der Freundesliste entfernen, doch kann eine leere Liste nicht gespeichert werden.

5. Um Ihre Freunde über den SIM-Kartenwechsel auf Ihrem Telefon zu benachrichtigen, aktivieren Sie die Option **Freunde über Wechsel der SIM-Karte benachrichtigen**.
6. Damit der Versand von SMS-Befehlen von Rufnummern Ihrer Freunde ohne Eingabe des für den **Dr.Web Dibstahlschutz** festgelegten Passworts erlaubt wird, aktivieren Sie die Option **SMS-Befehle ohne Passwort erlauben**.



Unabhängig davon, ob die Option **SMS-Befehle ohne Passwort erlauben** gewählt ist oder nicht, können Ihre Freunde den Befehl **#RESETPASSWORD#** ohne Passwort an Ihr Telefon senden. Dieser Befehl dient zur Freischaltung des Telefons und Zurücksetzung des Passworts für den **Dr.Web Dibstahlschutz**.

Auf Geräten unter Android 4.4 und höher kann die Option **SMS-Befehle ohne Passwort erlauben** nicht deaktiviert werden.

SMS-Befehle

Die Verwaltung vom **Dr.Web Dibstahlschutz** erfolgt über spezielle SMS-Befehle. Diese Befehle ermöglichen es Ihnen, Ihr Telefon zu orten sowie seine Funktionen zu sperren und Ihre persönliche Daten zu löschen.

Tabelle der SMS-Befehle

Zur Verwaltung vom **Dr.Web Dibstahlschutz** können Sie folgende SMS-Befehle verwenden:

Befehl	Aktion
#SIGNAL#Passwort#	Telefon sperren und ein Tonsignal darauf aktivieren, das auch nach dem Neustart des Telefons erklingen wird.
#LOCK#Passwort#	Telefon sperren.
#UNLOCK#Passwort#	Telefon ohne Zurücksetzung des Passworts für den Dr.Web Dibstahlschutz freischalten.
#LOCATE#Passwort#	GPS-Koordinaten des Telefons in einer SMS-Nachricht erhalten. Die erhaltene SMS-Nachricht wird einen Link zur Karte mit vermutlichen Koordinaten Ihres Geräts beinhalten. Wenn Sie dem erhaltenen Link folgen, wird der Standort Ihres Geräts mit Hilfe vom Dr.Web Dibstahlschutz Locator angezeigt. Es ist ein spezieller Dienst von Doctor Web, der eine Karte und den Standort Ihres Geräts darauf im Fenster des Webbrowsers anzeigen lässt. Die Genauigkeit bei der Ortung des Geräts hängt von verfügbaren GPS-Empfängern, sichtbaren Wi-Fi-Netzwerken sowie von den nächstgelegenen GSM-Basisstationen ab. Je nach erhaltenen Daten wird der Standort genau (als eine Position auf der Karte) bzw. ungefähr (als ein Kreis bestimmter Größe) bestimmt. Im oberen Bereich des Bildschirms mit Karte können Sie den gewünschten Ortungsdienst wählen.



Befehl	Aktion
#WIPE#Passwort#	Telefon auf die Werkseinstellungen zurücksetzen und alle Daten von der SD-Karte löschen. Dieser Befehl wird auch nach 10-maliger falscher Passworteingabe ausgeführt, falls das Telefon gesperrt ist und die Option Daten nach zehnmaliger Eingabe eines falschen Passwortes löschen in den Einstellungen vom Dr.Web Diebstahlschutz ausgewählt wurde.
#RESETPASSWORD#	Telefon freischalten und das für den Dr.Web Diebstahlschutz festgelegte Passwort zurücksetzen. Dieser Befehl kann nur von einer Rufnummer, die auf der Freundesliste ist, gesendet werden.



Bei SMS-Befehlen wird die Groß-/Kleinschreibung nicht beachtet. Beispielsweise können Sie den Befehl **#LOCK#Passwort#** in Form von **#Lock#Passwort#**, **#lock#Passwort#**, **#lOck#Passwort#** usw. senden, um das Telefon zu sperren.

Zur Genauigkeit der nach dem Versand des SMS-Befehls **#LOCATE#** erhaltenen Ergebnisse erlauben Sie die Nutzung drahtloser Netzwerke in den Einstellungen Ihres Gerätes bei seiner Ortung.

SMS-Befehle über die Oberfläche vom Dr.Web Diebstahlschutz senden

Sie können SMS-Befehle direkt über die Oberfläche vom **Dr.Web Diebstahlschutz** an andere Telefone, die auch mit dem **Dr.Web Diebstahlschutz** eingerichtet sind, versenden. Dafür müssen Sie wie folgt vorgehen:

1. Tippen Sie auf dem Einstellungsbildschirm des **Dr.Web Diebstahlschutzes** (s. [Abbildung 11](#)) unter **Freunde** auf **SMS-Befehle senden**.
2. Geben Sie die Rufnummer ein, an die Sie einen SMS-Befehl senden wollen.
3. Wählen Sie einen Befehl aus der Liste aus:
 - **Sperren** – entspricht dem Befehl [#LOCK#](#)
 - **Sperren und Tonsignal aktivieren** – entspricht dem Befehl [#SIGNAL#](#)
 - **Freischalten** – entspricht dem Befehl [#UNLOCK#](#)
 - **Alle Daten löschen** – entspricht dem Befehl [#WIPE#](#)
 - **Lage feststellen** – entspricht dem Befehl [#LOCATE#](#)
 - **Passwort zurücksetzen** – entspricht dem Befehl [#RESETPASSWORD#](#)
4. Geben Sie das für **Dr.Web Diebstahlschutz** auf dem Telefon des Befehlsempfängers festgelegte Passwort ein. Wenn Ihre Rufnummer der Freundesliste des Befehlsempfängers hinzugefügt ist, brauchen Sie das Passwort nicht einzugeben.
5. Tippen Sie auf **Senden**.

Dr.Web Diebstahlschutz-Sperre aufheben

Sollten Sie Ihr für den **Dr.Web Diebstahlschutz** definiertes Passwort vergessen haben, führen Sie folgende Aktionen aus:

1. Besuchen Sie die Webseite <https://antitheft.drweb.com/>.
2. Geben Sie in den entsprechenden Feldern den Code, der auf dem Bildschirm des gesperrten Gerätes erscheint, sowie die E-Mail-Adresse, die zur Registrierung des **Dr.Web Diebstahlschutzes** auf dem Server von **Doctor Web** verwendet wurde, ein (s. [Abbildung 12](#)).
3. Betätigen Sie die Schaltfläche **Code erhalten**. An die angegebene E-Mail-Adresse wird ein spezieller Code zur Entsperrung Ihres mobilen Endgeräts und Deaktivierung vom **Dr.Web Diebstahlschutz** gesendet.
4. Geben Sie ins Eingabefeld **Geben Sie das Diebstahlschutz-Passwort ein** auf dem Bildschirm des gesperrten mobilen Endgeräts den zugesendeten Code ein.



Ihr mobiles Endgerät ist nun entsperrt und der Dr.Web Diebstahlschutz ist deaktiviert. Um den **Dr.Web Diebstahlschutz** erneut zu aktivieren, müssen Sie das Programm neu starten und alle notwendigen Einstellungen vornehmen.

Geben Sie das Diebstahlschutz-Passwort ein

Dieses mobile Endgerät ging möglicherweise verloren oder wurde gestohlen. Sie können Kontakt mit dem Eigentümer über die E-Mail-Adresse user@mail.com aufnehmen. Eine Belohnung ist garantiert.

Haben Sie Ihr Passwort vergessen?

Sind Sie der Besitzer des Telefons und haben das Passwort vergessen, führen Sie eine der folgenden Aktionen durch:

- senden Sie an Ihr Telefon eine SMS-Nachricht mit dem Befehl #UNLOCK# von einer Nummer, die Ihrer Freundesliste hinzugefügt ist;
- öffnen Sie die Seite <https://antitheft.drweb.com> und geben Sie den Code **KPVDJFGKDHCTHRJMB** und die E-Mail-Adresse **user@mail.com** in die entsprechenden Eingabefelder ein. Der Code für die Zurücksetzung des Passworts und Deaktivierung

OK

Code zur Entsperrung von Dr.Web Diebstahlschutz erhalten

Wenn Sie Ihr Passwort für Dr.Web Diebstahlschutz vergessen haben, gehen Sie so vor:

1. Klicken Sie auf **Haben Sie Ihr Passwort vergessen?** auf dem Bildschirm Ihres gesperrten Geräts.
2. Geben Sie in die unten stehenden Felder den Code und die E-Mail-Adresse ein, die auf dem Bildschirm Ihres gesperrten Geräts angezeigt werden.
3. Klicken Sie die Schaltfläche **Code erhalten** an. An die angegebene E-Mail-Adresse wird ein einmaliger Code zur Entsperrung Ihres Geräts versendet.

[Mehr](#)

Code auf dem Bildschirm des gesperrten Geräts:

E-Mail-Adresse:

Code erhalten

Abbildung 12. Dr.Web Diebstahlschutz-Sperre aufheben

Zugriff auf Internet-Inhalte einschränken

Der Zugriff auf Internet-Inhalte wird mit einem speziellen URL-Filter **Cloud Checker** kontrolliert. Damit wird der Benutzer des mobilen Geräts vor unerwünschten Web-Inhalten geschützt.



Mit **Cloud Checker** wird der Zugriff auf Web-Inhalte nur beim integrierten Android-Browser sowie dem Browser Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser bzw. Boat Browser Mini kontrolliert.

Im **Zentralschutz-Modus** können die Einstellungen der Komponente **Cloud Checker** entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein.

Der Filter **Cloud Checker** ermöglicht Ihnen, den Zugriff auf die folgenden Kategorien unerwünschter und potentiell gefährlicher Webseiten zu sperren:

- Nicht empfohlene Websites
- Websites für Erwachsene
- Gewalt
- Waffen
- Glücksspiele
- Drogen
- Anstößige Sprache
- Chats



- Terrorismus
- E-Mail
- Soziale Netzwerke
- Auf Antrag des Rechtsinhabers.

Der Filter **Cloud Checker** blockiert standardmäßig Zugriff auf die Webseiten, die als Gefahrenquelle bekannt sind.



Damit **Cloud Checker** funktionsfähig sein kann, müssen Sie in Ihrem jeweiligen Webbrowser den Browserverlauf aktivieren.

URL-Filter aktivieren/deaktivieren

1. Auf dem Hauptbildschirm der Anwendung (s. [Abbildung 2](#)) wählen Sie **Cloud Checker**. Es öffnet sich der Bildschirm mit Einstellungen für den URL-Filter (s. [Abbildung 13](#)).

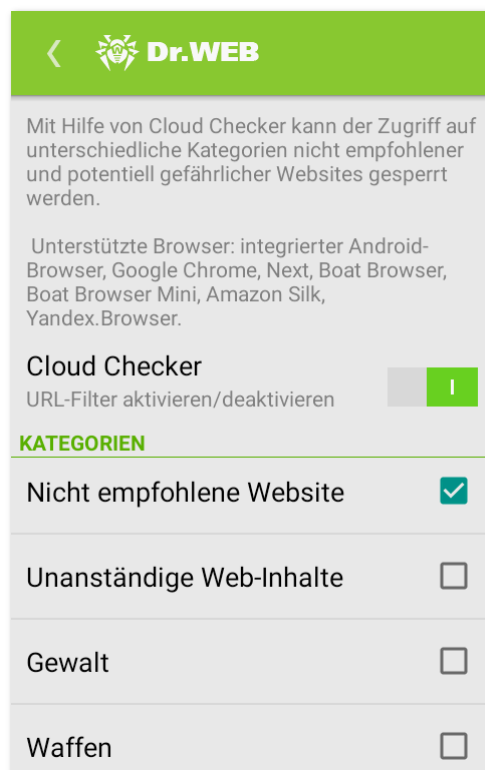


Abbildung 13. Bildschirm mit Einstellungen für Cloud Checker

2. Filtern der Internet-Inhalte wird mit der Option **Cloud Checker** aktiviert/deaktiviert. Standardmäßig ist Filtern der Internet-Inhalte aktiv.
3. In der Liste **Kategorien** wählen Sie die Kategorien von Websites aus, auf welche Sie den Zugriff sperren wollen.

Dr.Web Firewall

Die **Dr.Web Firewall** ist für den Schutz Ihres mobilen Geräts vor unbefugtem Zugang von außen bestimmt und beugt dem Verlust wichtiger Daten im Netzwerk vor. Diese Komponente gestattet es Ihnen, die Verbindungen und Datenübertragung im Internet zu überwachen sowie verdächtige Verbindungen zu sperren.



Die **Dr.Web Firewall** nutzt die VPN-Technologie für Android. Bei manchen Geräten kann das VPN-Protokoll vom Hersteller deaktiviert werden und für andere Anwendungen nicht zugänglich sein. In diesem Fall sind die Firewall-Funktionen nicht verfügbar. Für weitere Informationen kontaktieren Sie den Hersteller Ihres mobilen Geräts.

Dr.Web Firewall aktivieren/deaktivieren

1. Auf dem Hauptbildschirm der Anwendung (s. [Abbildung 2](#)) wählen Sie die Option **Firewall**. Es öffnet sich der Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)).

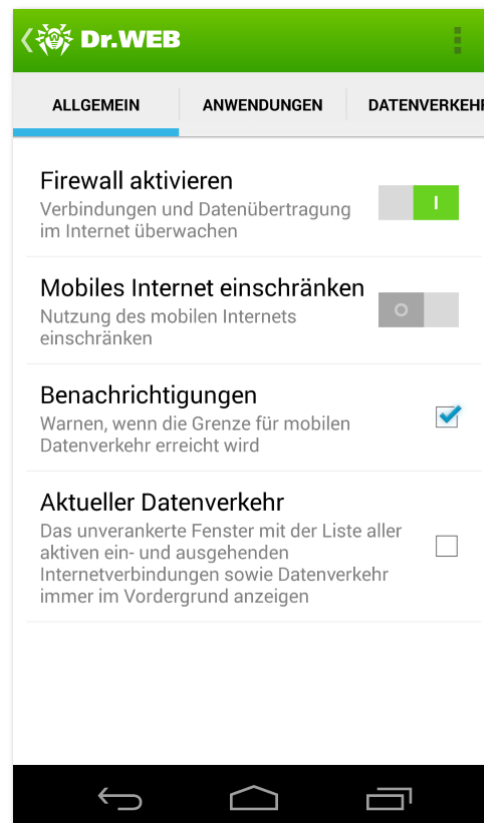


Abbildung 14. Einstellungsbildschirm der Firewall. Registerkarte Allgemein

2. Das Aktivieren/Deaktivieren der Firewall erfolgt mit Hilfe der Option **Firewall aktivieren**. Standardgemäß ist die Firewall deaktiviert. Beim Aktivieren der Firewall wird der Benutzer angefordert, die VPN-Verbindungen für **Dr.Web** freizugeben. Sie müssen VPN erlauben, damit die Firewall funktioniert.



Wenn die Rechte für die VPN-Nutzung im Laufe der Arbeit auf eine andere Anwendung übergehen, wird die **Dr.Web Firewall** deaktiviert. In dem Benachrichtigungsbereich wird dabei die entsprechende Warnmeldung angezeigt. Um die **Dr.Web Firewall** wieder zu aktivieren, brauchen Sie nur auf diese Warnmeldung zu tippen.

Besonderheiten der Nutzung

Die **Dr.Web Firewall** wird auf der Basis der VPN-Technologie für Android realisiert und kann demgemäß funktionieren, ohne dass Superuser-Rechte (root) dafür benötigt werden. Die **Dr.Web Firewall** kann also auf einem beliebigen Gerät benutzt werden, sofern es unter Android 4.0 oder höher läuft. Es bestehen aber bestimmte Einschränkungen beim Realisieren der VPN-Technologie unter Android:

- VPN kann zu jedem Zeitpunkt nur von einer Anwendung auf dem Gerät benutzt werden. Wenn also



die Anwendung VPN aktiviert, öffnet sich dabei ein Fenster mit der Anforderung an Benutzer, VPN für diese Anwendung zu erlauben. Wenn der Benutzer es erlaubt, beginnt die Anwendung, VPN zu verwenden. Dabei aber wird VPN für eine andere Anwendung, die bisher VPN verwendete, verboten. Diese Anforderung wird beim ersten Aktivieren der **Dr.Web Firewall** sowie nach jedem Neustart angezeigt. Darüber hinaus kann diese Anforderung angezeigt werden, wenn andere Anwendungen VPN-Zugang beantragen. Die Verwendung von VPN wird also zwischen mehreren Anwendungen zeitlich verteilt und die Firewall kann nur dann funktionieren, wenn sie über alle VPN-Rechte verfügt.

- Die aktivierte **Dr.Web Firewall** verhindert möglicherweise, dass sich das von ihr geschützte mobile Gerät mit anderen Geräten direkt über WLAN oder LAN verbindet. Dies hängt jeweils vom Model des Geräts und von den Anwendungen ab, die für die Herstellung von Verbindungen verwendet werden.



Die VPN-Technologie für Android dient nur zur Realisierung der Firewall-Funktionen. Es wird dabei kein VPN-Tunnel eingerichtet, der Internet-Traffic wird nicht verschlüsselt.

Mobiles Internet einschränken

Mit Hilfe der **Dr.Web Firewall** können Sie die Grenze bei der Nutzung des mobilen Internets festlegen.

1. Um die Option für die Einschränkung des mobilen Internets zu aktivieren/deaktivieren, navigieren Sie zu **Mobiles Internet einschränken** auf der Registerkarte **Allgemein** im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)).
2. Beim Aktivieren dieser Option müssen Sie die Grenze für mobilen Datenverkehr setzen (in Megabytes oder Gigabytes). Sie können den Zeitraum festlegen, innerhalb dessen die Einschränkung gültig ist: ein Tag, eine Woche oder ein Monat.
3. Gegebenenfalls geben Sie das verbrauchte Traffic-Volumen ab Beginn der festgelegten Einschränkung der Internetnutzung an:
 - wenn ein Tag als Dauer der Einschränkung festgelegt wurde, wird die Zeit ab 00:00 des laufenden Tages berechnet;
 - wenn eine Woche als Dauer der Einschränkung festgelegt wurde, wird die Zeit ab 00:00 des laufenden Tages berechnet;
 - wenn ein Monat als Dauer der Einschränkung festgelegt wurde, wird die Zeit ab 00:00 des ersten Tages des laufenden Kalendermonats berechnet.

Wenn die Einschränkung der Nutzung des mobilen Internets aktiviert wird, wird ein Diagramm mit Informationen zum verbleibenden Traffic auf der Registerkarte **Allgemein** im Einstellungsbildschirm der Firewall angezeigt. Daneben finden Sie auch die Angaben zur festgelegten Traffic-Grenze und einen Counter, der die Zeit bis zum Ablauf der Einschränkung rückwärts zählt (s. [Abbildung 15](#)).

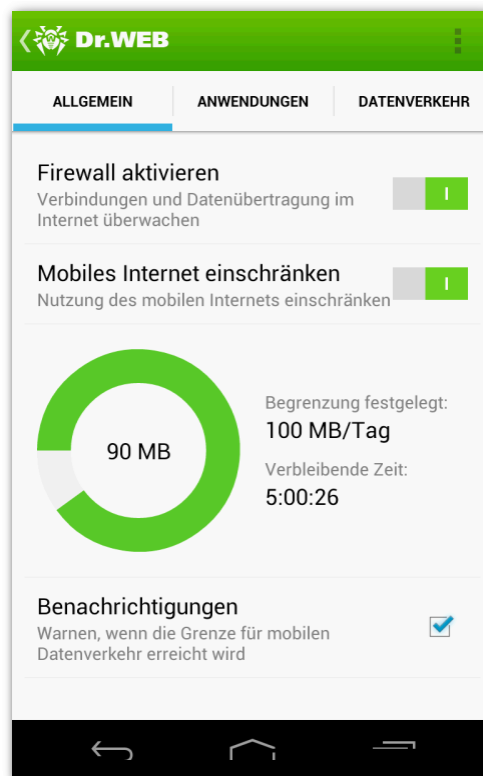


Abbildung 15. Einstellungsbildschirm der Firewall mit aktivierter Option zur Einschränkung des mobilen Internets



Beim Einschränken des mobilen Datenverkehrs ist eine geringe Überschreitung von max. 4 KB erlaubt.

Benachrichtigungen

Sie können die Benachrichtigungen über das Erreichen der festgelegten Grenze für mobilen Datenverkehr konfigurieren. Dazu markieren Sie das Kontrollkästchen bei **Benachrichtigungen** auf der Registerkarte **Allgemein** im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)).

Anwendungsdatenverkehr behandeln

Die **Dr.Web Firewall** ermöglicht es Ihnen, die Behandlung des Internetdatenverkehrs auf Anwendungsebene zu konfigurieren, sodass Sie den Zugriff bestimmter Programme und Prozesse auf die Netzwerkressourcen überwachen können. Die Informationen zum Internetdatenverkehr, der von den auf Ihrem Gerät installierten Anwendungen verwendet wird, finden Sie auf der Registerkarte **Anwendungen** im Einstellungsbildschirm der Firewall. Hier können Sie auch die Zugriffsregeln auf die Netzwerkressourcen für die Anwendungen einstellen (s. [Abbildung 16](#)).

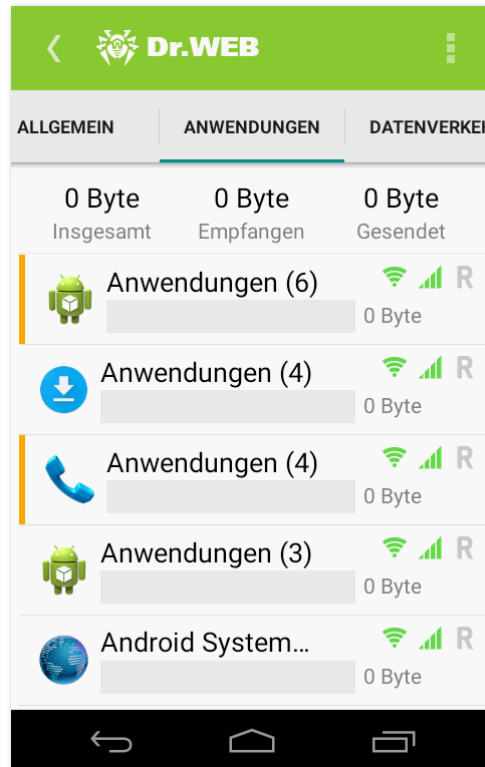


Abbildung 16. Einstellungsbildschirm der Firewall. Registerkarte Anwendungen

Auf der Registerkarte **Anwendungen** wird die Gesamtzahl der im Netzwerk übertragenen Daten sowie das Volumen des empfangenen und gesendeten Traffics angezeigt.

Nachstehend finden Sie eine Liste der Anwendungen (und Anwendungsgruppen) mit Angabe des verbrauchten Internettraffics für jede davon. Um die Liste aller auf dem Gerät installierten Anwendungen, einschließlich der Anwendungen, deren Traffic-Verbrauch null beträgt, anzeigen zu lassen, aktivieren Sie das Kontrollkästchen **Alle Anwendungen** im Menü auf der Registerkarte **Anwendungen**.

Für jede Anwendung können Sie die Nutzung von Wi-Fi, mobilem Internet und Internet im Roaming anhand der entsprechenden Optionen, die rechts von dem Anwendungsnamen untergeordnet sind, erlauben/verbieten.



Anwendungen, deren Einstellungen geändert wurden, werden hervorgehoben.

Um detaillierte Informationen zur Internetnutzung durch eine Anwendung (Anwendungsgruppe) in der Liste einzusehen, tippen Sie darauf. Im geöffneten Fenster sind folgende Optionen verfügbar:

- die Nutzung von Wi-Fi, mobilem Internet und Internet im Roaming der Anwendung (Anwendungsgruppe) erlauben/verbieten;
- das [Protokoll](#) der Anwendung (Anwendungsgruppe) einsehen;
- die [Statistik](#) für die Nutzung des Internetdatenverkehrs durch diese Anwendung (Anwendungsgruppe) einsehen;
- die [Regeln für Behandlung von Verbindungen](#) für die ausgewählte Anwendung (Anwendungsgruppe) einstellen.

Statistik zur Nutzung des Internet-Datenverkehrs

Auf dem Bildschirm mit detaillierten Informationen zum Datenverkehr einer Anwendung (Anwendungsgruppe) können Sie die grafisch dargestellte Statistik zur Internetnutzung durch diese Anwendung einsehen (s. [Abbildung 17](#)).

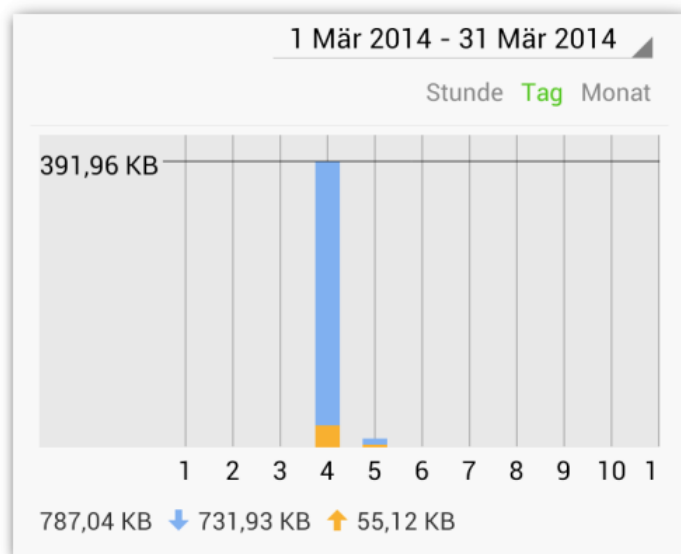


Abbildung 17. Statistik zur Nutzung des Internettraffics durch die Anwendung

Gelb ist der ausgehende Datenverkehr, blau ist der eingehende Datenverkehr im Diagramm markiert. Unter dem Diagramm sind die Zahlenwerte für verbrauchten Traffic (gesamt, ausgehend und eingehend) angeführt.

Beim Einsehen der Statistiken zur Nutzung des Internet-Datenverkehrs können Sie folgende Aktionen durchführen:

- Einen Zeitabstand zum Einsehen der Statistik in der entsprechenden Liste auswählen. Es stehen Ihnen die statistischen Daten für den laufenden Tag, die letzte Woche, den laufenden Monat und den vorherigen Monat zur Verfügung. Sie können auch selbständig einen Zeitabstand definieren. Dazu geben Sie das Anfangs- und Endedatum an.
- Innerhalb des ausgewählten Zeitabstandes können die Statistiken nach Stunden, Tagen oder Monaten angezeigt werden.

Statistik bereinigen

Gegebenenfalls können Sie die ganze Statistik zum Betrieb der Firewall bzw. die Statistik für einzelne Anwendungen leeren.

Um die Statistik für alle Anwendungen zu löschen:

1. Auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)) wählen Sie die Option **Bereinigen** im Menü aus.



2. In dem geöffneten Fenster aktivieren Sie das Kontrollkästchen **Statistik bereinigen**. Tippen Sie auf **OK**.

Um die Statistik für eine bestimmte Anwendung zu löschen:

1. Auf der Registerkarte **Anwendungen** im Einstellungsbildschirm der Firewall (s. [Abbildung 16](#)) wählen Sie die Anwendung, deren Statistik zu löschen ist, aus.
2. Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung wählen Sie die Option **Bereinigen** im Menü aus.
3. In dem geöffneten Fenster aktivieren Sie das Kontrollkästchen **Statistik für diese Anwendung bereinigen**. Tippen Sie auf **OK**.

Verbindungsregeln

Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung (Anwendungsgruppe) können Sie auch die Regeln für die Verbindung dieser Anwendung zu bestimmten IP-Adressen und Ports festlegen.

Einen Regelsatz erstellen

1. Um eine Regel zu erstellen, tippen Sie auf **Regel hinzufügen**. Sie können erlaubende und verbotende Regeln je nach Auswahl einer entsprechenden Option im Bereich **Verbindungsregeln** hinzufügen:
 - wenn **Verbindungen in der Liste sperren** ausgewählt ist, wird eine verbotende Regel hinzugefügt.
 - wenn **Nur Verbindungen in der Liste erlauben** ausgewählt ist, wird eine erlaubende Regel hinzugefügt
2. Im Fenster zur Regelerstellung im Feld **IP-Adresse** geben Sie eine gültige IP-Adresse (im Format a.b.c.d), IP-Adressenbereich (im Format a1.b1.c1.d1-a2.b2.c2.d2) oder das ganze Netzwerk (im Format a.b.c.0/n, wobei n - eine Zahl von 1 bis 32) an oder lassen Sie das Feld leer (in diesem Fall müssen Sie den Verbindungsport unbedingt festlegen). Im Feld **Port** geben Sie die Nummer eines gültigen Ports an oder lassen Sie das Feld leer (in diesem Fall müssen Sie die IP-Adresse der Verbindung unbedingt festlegen). Wenn eines der Felder leer geblieben ist, gilt die Regel für beliebige IP-Adressen oder Ports. Tippen Sie auf **OK**, um erstellte Regel zu speichern.
3. Um eine bestehende Regel zu bearbeiten, tippen Sie auf diese Regel in der Liste und halten Sie diese gedrückt, dann tippen Sie auf **Editieren**.

Außerdem können Sie bei der Anzeige der [Protokolle von Anwendungen](#) oder der Liste [aktiver Verbindungen](#) erlaubende bzw. verbotende Regeln hinzufügen.

Verbindungsregeln löschen

- Um eine Regel zu löschen, tippen Sie in der Liste darauf und halten Sie diese gedrückt, dann tippen Sie auf **Löschen**.
- So löschen Sie alle Regeln für eine Anwendung
 1. Wählen Sie in der Liste die gewünschte Anwendung (s. [Abbildung 16](#)) aus.
 2. Wählen Sie im Menü der App den Punkt **Bereinigen**.
 3. Setzen Sie im geöffneten Fenster das Häkchen bei **Regeln für diese Anwendungen löschen**.
- So löschen Sie alle Regeln für alle Anwendungen
 1. Öffnen Sie auf dem Bildschirm mit der Liste aller Anwendungen das Menü der App (s. [Abbildung 16](#)) und wählen Sie dann **Bereinigen** aus.
 2. Setzen Sie im geöffneten Fenster das Häkchen bei **Regeln für Anwendungen löschen**.

Eingehende Verbindungen

Das Kontrollkästchen **Eingehende Verbindungen erlauben** im Menü auf dem Bildschirm mit Informationen zum Anwendungstraffik ermöglicht es Ihnen, eingehende Verbindungen von der Prüfung



durch die Firewall auszunehmen. Die Information zu den Verbindungen, die von beliebigen Remote-Adressen mit dem durch diese Anwendung geöffneten Port initiiert wurden, wird in dem [Anwendungsprotokoll](#) und der [Statistik](#) zum Betrieb der Firewall nur teilweise angeführt. Des Weiteren können beliebige Verbindungen mit diesen Adressen von der Prüfung durch die Firewall auch für andere Anwendungen ausgenommen werden. Ein solcher Modus ist nicht sicher, und es wird nicht empfohlen, diesen im allgemeinen Fall zu verwenden.

Es ist sinnvoll, eingehende Verbindungen zuzulassen, wenn die Firewall auf keine andere Weise deaktiviert werden kann. Das kann beispielsweise der Fall sein, wenn auf dem Gerät ein Server, der Verbindungen von externen Netzwerken empfängt, eingerichtet ist.

Aktuelle Aktivität der Netzwerkverbindungen

Sie können Informationen zur aktuellen Aktivität von Netzwerkverbindungen über die folgenden Wege erhalten:

1. Auf der Registerkarte **Datenverkehr** im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)).

Auf der Registerkarte **Datenverkehr** wird eine Liste der Verbindungen, die durch die auf dem Gerät installierten Anwendungen initiiert wurden, in Echtzeit angezeigt. Um detaillierte Informationen zu Verbindungen einer Anwendung (IP-Adressen und Ports der Verbindungen sowie das Volumen des gesendeten/empfangenen Datenverkehrs) anzeigen zu lassen, tippen Sie in der Liste darauf.

Sie können erlaubende bzw. verbotende Regeln für die Anwendungen in der Liste erstellen. Tippen und halten Sie die Verbindung in der Liste gedrückt, danach wählen Sie die entsprechende Option aus:

- **Erlaubende Regel hinzufügen**, um eine Regel zu erstellen, die Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port erlaubt;
- **Verbotende Regel hinzufügen**, um eine Regel zu erstellen, die alle Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port sperrt.

2. Im unverankerten Fenster mit Informationen zum aktuellen Datenverkehr.

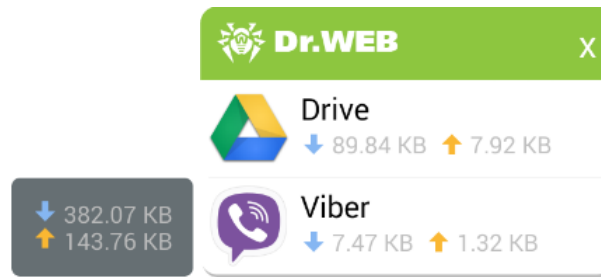
Um das Fenster anzeigen zu lassen, aktivieren Sie das Kontrollkästchen **Aktueller Datenverkehr** im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)). Im Vordergrund vor allen anderen Anwendungen wird das Fenster mit der Liste aller aktiven ein- und ausgehenden Internetverbindungen sowie der Datenverkehr (s. [Abbildung 18a](#)) angezeigt.



Beim angezeigten Datenverkehrsvolumen handelt es sich um das Datenverkehrsvolumen, das erst nach dem Öffnen des Fensters gemessen wird.

Unverankertes Fenster verwenden

- Um die Liste mit allen Anwendungen, die Ihre Internetverbindung verwenden (s. [Abbildung 18b](#)), aufzurufen, tippen Sie auf das unverankerte Fenster. Bei der Auswahl einer Anwendung wird die Registerkarte **Datenverkehr** geöffnet, in der detaillierte Informationen zu aktuellen Verbindungen angezeigt werden.
- Um die Liste mit den Anwendungen zu schließen, tippen Sie auf **X**.
- Um das Fenster auszublenden, deaktivieren Sie das Kontrollkästchen **Aktueller Datenverkehr**.



Abbildungen 18a und 18b. Unverankertes Fenster mit aktuellem Datenverkehr

Ereignisse registrieren

Die App protokolliert Ereignisse für die **Dr.Web Firewall**. Sie können die [gesamte Liste der Ereignisse](#) oder nur die Ereignisse, die mit Nutzung des Internet-Traffics durch einzelne [Anwendungen](#) verbunden sind, einsehen.

Protokoll der Dr.Web Firewall

Um die Liste aller Ereignisse, die mit dem Betrieb der **Dr.Web Firewall** verbunden sind, anzeigen zu lassen, wählen Sie die Option **Protokoll** im Menü auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall aus (s. [Abbildung 14](#)).

Ereignisprotokoll anzeigen lassen

Damit die Suche nach Informationen einfacher wird, können Sie die Sortierung der Einträge und schnelles Scrollen (durch Bewegen eines speziellen grafischen Elementes im rechten Bildschirmbereich) beim Einsehen der Ereignisliste verwenden. Zur Sortierung der Einträge im Protokoll wählen Sie das Sortierungskriterium im Menü auf dem Protokoll-Bildschirm.

Es werden folgende Informationen für jedes Ereignis im Protokoll angezeigt:

- Datum und Zeit der Verbindung (für TCP) bzw. Zeitraum, innerhalb dessen die Datenpakete mit entsprechenden Traffic-Werten empfangen wurden (für UDP). Zum Beispiel: 18/02/2014 2:07:11 - 18/02/2014 2:07:12.
- Lokale Adresse und lokaler Port. Zum Beispiel: src: 10.2.3.5:6881.
- Eingehender und ausgehender Datenverkehr (in Bytes) bzw. Anzahl der gesperrten Pakete. Zum Beispiel: in:103 out:112 oder blocked packets:1.
- ID einer Anwendung auf dem Gerät, die mit diesem Datenverkehr assoziiert ist (User ID). Zum Beispiel: uid=10071.
- Anzahl an Datenverkehrsstaus (nur für TCP). Zum Beispiel: traffic jam=0. Datenverkehrsstau ist eine Situation, wenn das Client-Programm den TCP-Pufferspeicher nicht rechtzeitig entladen kann. Dabei entsteht ein Stau, durch den die Datenübertragung im Netzwerk langsamer werden kann.

Protokoll bereinigen

Um alle Ereignisse, die mit dem Betrieb der **Dr.Web Firewall** verbunden sind, aus der Liste zu löschen, müssen Sie wie folgt vorgehen:

1. Auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)) wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster aktivieren Sie das Kontrollkästchen **Protokoll bereinigen**. Tippen Sie auf **OK**.



Protokollgröße

Standardmäßig beträgt die maximale Größe der Protokolldatei 5 MB. Um die maximale Größe der Protokolldatei zu ändern, müssen Sie wie folgt vorgehen:

1. Auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall (s. [Abbildung 14](#)) wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster ändern Sie den Wert, der im Feld **Maximale Größe der Protokolldatei** angegeben ist. Tippen Sie auf **OK**.

Anwendungsprotokolle

Um die Liste der Ereignisse einzusehen, die mit den Netzwerkverbindungen einer Anwendung auf Ihrem Gerät verbunden sind, tippen Sie auf **Protokoll** auf dem Bildschirm mit detaillierter Information zum Datenverkehr dieser Anwendung.

Anwendungsprotokoll anzeigen lassen

Alle Ereignisse für eine bestimmte Anwendung sind nach Datum im Protokoll vereinigt. Um die Ereignisliste zu einem bestimmten Datum anzeigen zu lassen, tippen Sie in der Liste darauf. Es werden folgende Informationen zu jedem Ereignis angezeigt:

- Verbindungszeit (für TCP) oder der Zeitraum, innerhalb dessen die Datenpakete mit entsprechenden Traffic-Werten empfangen wurden (für UDP);
- lokale Adresse und lokaler Port;
- eingehender und ausgehender Datenverkehr (in Bytes) bzw. Anzahl der gesperrten Pakete;

Sie können erlaubende bzw. verbotende Regeln für die Verbindungen im Anwendungsprotokoll erstellen. Tippen Sie und halten Sie die Verbindung in der Liste gedrückt, danach wählen Sie die entsprechende Option aus:

- **Erlaubende Regel hinzufügen**, um eine Regel zu erstellen, die Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port erlaubt;
- **Verbotende Regel hinzufügen**, um eine Regel zu erstellen, die alle Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port sperrt.

Anwendungsprotokoll bereinigen

Um das Anwendungsprotokoll zu bereinigen, müssen Sie wie folgt vorgehen:

1. Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster aktivieren Sie das Kontrollkästchen **Protokoll für diese Anwendung bereinigen**. Tippen Sie auf **OK**.

Registrierung von Ereignissen für eine Anwendung deaktivieren

Gegebenenfalls können Sie die Protokollierung für manche Anwendungen deaktivieren. Dafür müssen Sie wie folgt vorgehen:

1. Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster aktivieren Sie das Kontrollkästchen **Protokollierung für diese Anwendung deaktivieren**. Tippen Sie auf **OK**.

Bei Beseitigung der Sicherheitslücken helfen

Dr.Web ermöglicht die Diagnose und Analyse der Sicherheit von Ihrem Gerät. Die erkannten



Sicherheitsprobleme und -lücken lassen sich mit Hilfe einer speziellen Komponente - **Security Auditor** - beheben. Die Komponente startet automatisch, sobald die Anwendung zum ersten Mal gestartet und die Lizenz registriert wird. Die Anzahl erkannter Probleme wird im Bereich **Security Auditor** auf dem Hauptbildschirm der Anwendung angezeigt.



Wenn der **Security Auditor** bei der Analyse des Systems keine Sicherheitsprobleme und -lücken entdeckt, wird der entsprechende Bereich auf dem Hauptbildschirm der Anwendung nicht angezeigt.

Mögliche Probleme und deren Beseitigung

Sie können die Liste erkannter Sicherheitsprobleme einsehen (s. [Abbildung 19](#)). Tippen Sie dazu auf den Bereich **Security Auditor** auf dem Hauptbildschirm der Anwendung.

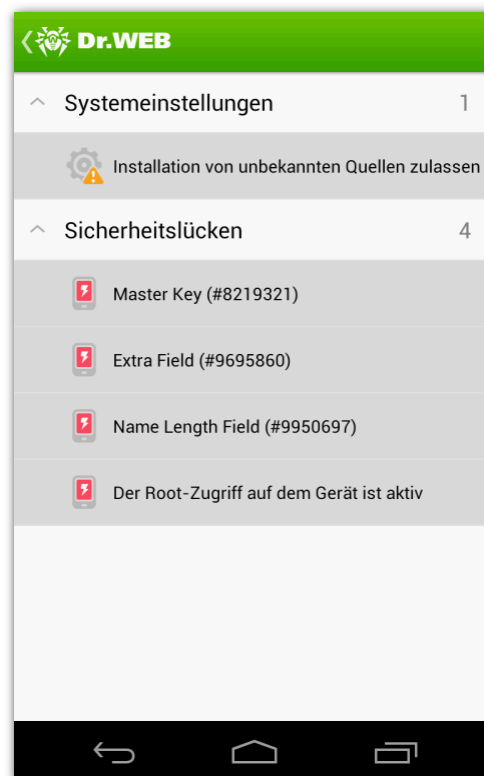


Abbildung 19. Liste der Sicherheitslücken, die im Gerät erkannt wurden

Mit **Dr.Web** können folgende Sicherheitsprobleme aufgedeckt werden: Anwendungen mit höchster Priorität bei Behandlung von SMS-Nachrichten, ausgeblendete Geräteadministratoren, Sicherheitslücken und Systemeinstellungen, die Sicherheit Ihres Geräts gefährden. Um detaillierte Informationen zu einem Problem und mögliche Beseitigungswege einzusehen, öffnen Sie die Liste von entsprechender Kategorie und tippen Sie auf das Sicherheitsproblem/-lücke in der Liste.

Anwendungen mit höchster Priorität bei Behandlung von SMS-Nachrichten

Diese Kategorie beinhaltet eine Liste von Anwendungen, die über eine höhere Priorität als **Dr.Web** beim Behandeln von SMS-Nachrichten verfügen. Solche Anwendungen können die Funktion von [Dr.Web Diebstahlschutz](#) und [Filtern der SMS-Nachrichten](#) sperren, da sie alle eingehenden Nachrichten und [Befehle](#) als erste behandeln. In manchen Fällen gehören diese Anwendungen zu Malware und können die Sicherheit Ihres Geräts gefährden.

Sollten Sie gemerkt haben, dass die Nachrichten nicht gefiltert werden bzw. der **Dr.Web Diebstahlschutz** nicht funktioniert, können Sie eventuell versuchen, entsprechende Einstellungen von Anwendungen auf der Liste zu bearbeiten. Die Anwendungen werden aus der Liste der



Sicherheitslücken entfernt. Wenn Sie nicht sicher sind, dass diese Anwendungen absolut vertrauenswürdig sind, empfiehlt es sich, diese zu entfernen. Um eine Anwendung zu entfernen, tippen Sie auf **Löschen** in dem Bereich mit detaillierten Informationen zum entstandenen Problem bzw. verwenden Sie das Standardverfahren des Betriebssystems.

Ausgeblendete Geräteadministratoren

Manche Anwendungen werden als Geräteadministratoren aktiviert, dabei aber werden sie in der Liste der Administratoren in den Geräteeinstellungen nicht angezeigt. Diese Anwendungen können mit Standardverfahren des Betriebssystems nicht entfernt werden. Es ist höchstwahrscheinlich, dass solche Anwendungen die Sicherheit Ihres Geräts gefährden können.

Sollten Sie nicht wissen, warum die Anwendung in der Liste der Geräteadministratoren ausgeblendet wird, empfiehlt es sich, diese zu entfernen. Um eine Anwendung zu entfernen, tippen Sie auf **Löschen** in dem Bereich mit detaillierten Informationen zum entstandenen Problem, das mit dieser Anwendung verbunden ist.

Systemeinstellungen

Zu Systemeinstellungen, die die Sicherheit des Geräts beeinflussen, gehören der Debugging-Modus sowie die Erlaubnis, die Anwendungen aus unbekannten Quellen zu installieren. Des Weiteren kann es gefährlich sein, die in Konflikt stehende Software zu benutzen:

- **USB-Debugging** ist der Entwicklermodus. Wenn Sie diesen Modus aktivieren, können Sie Daten vom Rechner auf Ihr Android-Gerät und umgekehrt kopieren, Apps installieren, Protokolldateien installierter Apps ansehen und eventuell löschen. Falls Sie kein Entwerfer sind und keinen Debugging-Modus verwenden, ist es empfehlenswert, diesen Modus zu deaktivieren. Um zum entsprechenden Bereich der Systemeinstellungen zu wechseln, tippen Sie auf dem Bildschirm, auf dem detaillierte Informationen zum Problem angezeigt werden, auf **Einstellungen**.
- Wenn Sie die **Installation von Apps aus unbekannten Quellen** zulassen, wird Ihr Android-Gerät viel mehr anfällig für bösartige Programme und Hackerattacke. Die nicht von Google Play Store heruntergeladenen Anwendungen können höchstwahrscheinlich gefährlich sein und die Sicherheit Ihres Geräts gefährden. Um das Risiko bei Installation von nicht sicheren Anwendungen zu reduzieren, empfiehlt es sich, die unbekannten Quellen zu verbieten. Um zum entsprechenden Bereich der Systemeinstellungen zu wechseln, tippen Sie auf dem Bildschirm, auf dem detaillierte Informationen zum Problem angezeigt werden, auf **Einstellungen**. Weiterhin ist es empfehlenswert, alle installierten Anwendungen auf Bedrohungen zu scannen. Vor Prüfungsbeginn stellen Sie sicher, dass die **Virendatenbanken** von **Dr.Web** [aktualisiert](#) sind.
- **Software-Konflikte**. Durch die Nutzung der in Konflikt stehenden Software, u.a. Browser, die durch den URL-Filter Cloud Checker nicht unterstützt werden, wird die Sicherheit des Geräts beeinträchtigt. Bei der Nutzung solcher Browser ist der Benutzer nicht vor unerwünschten und schädlichen Web-Ressourcen geschützt. Aus diesem Grund wird empfohlen, den integrierten Android-Browser als Default-Browser einzustellen und zu benutzen, Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser bzw. Boat Browser Mini.

Sicherheitslücken

Dr.Web findet im System des mobilen Geräts Sicherheitslücken wie Master Key (#8219321), Extra Field (#9695860), Name Length Field (#9950697), Fake ID (#13678484), ObjectInputStream Serialization (CVE-2014-7911), PendingIntent (CVE-2014-8609) und Android Installer Hijacking. Mittels dieser Sicherheitslücken können die böswilligen Benutzer den Programmcode manchen Anwendungen hinzufügen, ohne dass deren kryptographischen Signaturen geändert werden. Eine Folge davon ist, dass diese Anwendungen Funktionen, die die Sicherheit des Geräts gefährden werden, ausführen können. **Dr.Web** entdeckt auch die Heartbleed-Sicherheitslücke im System. Es ist ein Fehler in der kryptographischen OpenSSL-Software, der es den Böswilligen ermöglicht, den Zugriff auf die vertraulichen Angaben des Benutzers zu erhalten.

Wenn eine oder mehrere der genannten Sicherheitslücken entdeckt werden, überprüfen Sie, ob die



Updates für das Betriebssystem Ihres Geräts auf der Website des Herstellers vorhanden sind. Die Sicherheitslücken können in neuen Versionen bereits behoben werden. Sollten keine Updates verfügbar sein, empfiehlt es sich, die Anwendungen nur von vertrauenswürdigen Quellen zu installieren.

Weiterhin kann das Gerät durch unterschiedliche Typen der Bedrohungen gefährdet werden, wenn es gerootet ist, d.h. Änderungen vorgenommen wurden, welche mit Erlangen der Superuser-Rechte verbunden sind. Dadurch können die Systemdateien geändert bzw. gelöscht werden und das Gerät wird funktionsunfähig. Wenn Sie diese Änderungen selbständig vorgenommen haben, empfiehlt es sich, sie rückgängig zu machen. Wenn der Root-Zugriff auf Ihrem Gerät technisch bedingt ist bzw. zur Lösung bestimmter Aufgaben benötigt wird, seien Sie besonders vorsichtig, wenn Anwendungen aus unbekannten Quellen installiert werden.

Kurz-URL-Dienst

In manchen Fällen, z.B. bei begrenzter Anzahl von Zeichen in SMS-Nachrichten und sozialen Netzwerken, können kurz-URLs benötigt werden. **Dr.Web** ermöglicht es, Links zu kürzen und deren Inhalte mittels eines speziellen Kurz-Link-Dienstes zu überprüfen. Somit werden die Benutzer vor Virenbedrohungen geschützt.

Kurz-URL-Dienst nutzen

Um eine URL zu überprüfen und zu kürzen, gehen Sie wie folgt vor:

1. Markieren Sie die URL, die Sie überprüfen und kürzen möchten, und benutzen Sie die Browser-Funktion "Link senden".
2. Im geöffneten Menü wählen Sie den Punkt **URL verkürzen**. Die Webseite unter angegebener URL wird auf Bedrohungen gescannt. Wenn die Webseite sicher ist, wird die URL gekürzt und in die Zwischenablage kopiert. Sollte die Webseite Sicherheitsbedrohungen beinhalten, wird entsprechende Warnung von dem Dienst angezeigt.



Kapitel 6. Zentralschutz-Modus

Wenn Sie **Dr.Web** von der Website von **Doctor Web** installiert haben, können Sie das installierte Programm für Ihre Arbeit im Netzwerk, das über **Dr.Web Verwaltungszentrum** kontrolliert wird, oder auch für die Verbindung zum Antivirus-Dienst **Dr.Web AV-Desk**, der von Ihrem IT-Anbieter zur Verfügung gestellt wird, nutzen. Für den Virenschutz mit zentraler Verwaltung brauchen Sie keine zusätzlichen Plugins zu installieren bzw. das installierte **Dr.Web** Programm zu deinstallieren.



Die von Google Play installierte Version von **Dr.Web** verfügt über keinen Zentralschutz-Modus.

Durch Zentralschutz-Server verwaltete Komponenten

Einstellungen der Komponenten von **Dr.Web** können entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein.

Folgende Komponenten von **Dr.Web** können am Zentralschutz-Server verwaltet werden:

- [Dr.Web Scanner](#). Das Gerät kann dabei zeitgesteuert oder auf Anforderung des Nutzers gescannt werden. Ein Scanvorgang kann auch vom Zentralschutz-Server aus remote gestartet werden.
- [SpIDer Guard](#).
- [Anruf- und SMS-Filter](#).
- [Dr.Web Diebstahlschutz](#).
- [Cloud Checker](#).
- [Anwendungsfiler](#).

Lizenzierung im Zentralschutz-Modus

Die [Lizenzschlüsseldatei](#) wird vom Zentralschutz-Server automatisch bereitgestellt. Ihre private Lizenz wird dabei nicht verwendet. Wenn die aktuelle Lizenz abgelaufen ist oder gesperrt wurde, wenden Sie sich an den Administrator Ihres Antivirus-Netzwerkes, um eine neue gültige Lizenz zu erhalten, oder verlängern Sie Ihr Abo für **Dr.Web AV-Desk**.

Update im Zentralschutz-Modus

Im Zentralschutz-Modus ist das manuelle Update nicht möglich. Updates werden vom Zentralschutz-Server automatisch heruntergeladen. Update-Einstellungen können entsprechend der Sicherheitsrichtlinie des Unternehmens oder der Liste bezahlter Leistungen geändert oder gesperrt sein. Wenn der Zentralschutz-Server den mobilen Modus zulässt, können Sie beim Abbruch der Verbindung mit dem Zentralschutz-Server Virendatenbanken manuell aktualisieren.

In Zentralschutz-Modus wechseln

Um in den [Zentralschutz-Modus](#) zu wechseln, müssen Sie zuerst eine Verbindung mit dem Zentralschutz-Server herstellen.

Verbindung mit Eingabe von Verbindungsparametern

Um eine Verbindung mit dem Zentralschutz-Server herzustellen, brauchen Sie die



Verbindungsparameter, die Ihnen vom Administrator Ihres Antivirus-Netzwerks oder IT-Anbieter bereitgestellt werden.

Dafür müssen Sie wie folgt vorgehen:

1. Stellen Sie sicher, dass Sie eine stabile Netzwerkverbindung haben.
2. Setzen Sie auf dem Einstellungsbildschirm (s. [Abbildung 6](#)) im Bereich **Modus** das Häkchen neben **Dr.Web Agent**.



In der App, die mithilfe der vom Administrator des Antivirus-Netzwerks bereitgestellten Installationsdatei installiert wurde, ist die Option **Dr.Web Agent** standardmäßig aktiviert.

3. Beim Aktivieren des Zentralschutz-Modus werden die zuletzt gespeicherten Verbindungsparameter verwendet. Wenn Sie sich mit dem Zentralschutz-Server zum ersten Mal verbinden oder Ihre Verbindungsparameter geändert wurden, müssen Sie die folgenden Einstellungen festlegen:
 - IP-Adresse des Zentralschutz-Servers, die Ihnen der Administrator Ihres Antivirus-Netzwerks mitgeteilt hat.
 - Zusätzliche Einstellungen für die Autorisierung der Workstation: ID (Ihrem Gerät für die Registrierung am Server zugewiesen) und Passwort. Die Werte der obigen Einstellungen werden gespeichert und müssen bei erneuter Verbindung nicht noch einmal angegeben werden. Damit sich Ihr Gerät als Anfänger (neue Workstation) verbinden kann, öffnen Sie das Menü der App und wählen Sie die Option **Workstation als Anfänger verbinden**.
4. Tippen Sie auf **Verbinden**.

Verbindung mithilfe der Konfigurationsdatei

Einstellungen für die Verbindung mit dem Zentralschutz-Server sind in der Datei `install.cfg` enthalten, die Ihnen vom Administrator Ihres Antivirus-Netzwerks oder IT-Anbieter bereitgestellt wird.

Dafür müssen Sie wie folgt vorgehen:

1. Stellen Sie sicher, dass Sie eine stabile Netzwerkverbindung haben.
2. Legen Sie die Datei `install.cfg` in einem Stammordner oder einem Ordner der oberen Ebene auf der SD-Karte und im Gerätespeicher ab.
3. Setzen Sie auf dem Einstellungsbildschirm (s. [Abbildung 6](#)) im Bereich **Modus** das Häkchen neben **Dr.Web Agent**. Falls die Datei richtig abgelegt wurde, werden alle erforderlichen Eingabefelder automatisch ausgefüllt.



In der App, die mithilfe der vom Administrator des Antivirus-Netzwerks bereitgestellten Installationsdatei installiert wurde, ist die Option **Dr.Web Agent** standardmäßig aktiviert. Gleich nach der Installation sucht die App nach der Konfigurationsdatei und versucht anschließend, eine Verbindung mit dem Zentralschutz-Server herzustellen. Wenn die Datei nicht gefunden wurde oder falsche Verbindungsparameter enthält, müssen Sie das Häkchen neben **Dr.Web Agent** entfernen und erneut setzen und dann die erforderlichen Parameter manuell eingeben. Alternativ können Sie eine Konfigurationsdatei mit den richtigen Parametern verwenden.

4. Tippen Sie auf **Verbinden**.

Verbindungseinstellungen zurücksetzen

So setzen Sie Verbindungseinstellungen zurück



1. Öffnen Sie das Menü auf dem Bildschirm für die Eingabe der Verbindungsparameter.
2. Wählen Sie die Option **Verbindungseinstellungen zurücksetzen**.

Nach dem Zurücksetzen der Parameter wird die Datei `install.cfg`, welche die aktuellen Verbindungsparameter enthält, gelöscht. Wenn auf dem mobilen Gerät noch eine Konfigurationsdatei `install.cfg` vorhanden ist, werden alle erforderlichen Verbindungsparameter aus dieser Datei importiert. Aus diesem Grund werden die Verbindungseinstellungen erst dann zurückgesetzt, sobald alle Dateien `install.cfg` gelöscht werden.

Verbindungsfehler

Nicht unterstützte Option. Dieser Fehler tritt auf, wenn auf dem Server die Verschlüsselung und Komprimierung des Datenverkehrs verwendet werden, die von **Dr.Web** nicht unterstützt werden. Wenden Sie sich zur Behebung des Problems an den Administrator Ihres Antivirus-Netzwerkes oder Ihren IT-Anbieter.

Die Lizenz (das Abo) ist abgelaufen. Um sich mit dem Zentralschutz-Server verbinden zu können, müssen Sie sich an den Administrator Ihres Antivirus-Netzwerkes wenden, um eine gültige Lizenz zu erhalten, oder Ihr Abo für **Dr.Web AV-Desk** verlängern.

Das Abo wurde gesperrt. Um sich mit dem Zentralschutz-Server verbinden zu können, wenden Sie sich an den IT-Anbieter, der Ihnen **Dr.Web AV-Desk** zur Verfügung stellt, um die Sperre des Abos aufheben zu lassen.

Nicht verbunden. Der Zentralschutz-Server verweigert den Start von Dr.Web für Android. Dieser Fehler tritt auf, wenn Ihr Tarifplan die Verwendung von **Dr.Web** für Android nicht vorsieht oder **Dr.Web** für Android vom Administrator Ihres Antivirus-Netzwerkes gesperrt wurde.

Anwendungsfiler

Wenn die Einstellungen des Anwendungsfilters am Zentralschutz-Server geändert werden können, haben Sie die Möglichkeit, Ihre individuelle Liste der Anwendungen, die auf Ihrem mobilen Gerät gestartet werden dürfen, zu erstellen. Dafür müssen Sie wie folgt vorgehen:

1. Öffnen Sie auf dem Hauptbildschirm der App den Abschnitt **Administrator**.
2. Wählen Sie die Anwendungen aus, die auf Ihrem mobilen Gerät gestartet werden dürfen.
3. Tippen Sie auf **Ausgewähltes erlauben**. Die festgelegten Einstellungen werden an den Server übermittelt und als Ihre individuellen Einstellungen für Ihr Gerät gespeichert.

Als Administrator des Antivirus-Netzwerkes können Sie anhand Ihrer gespeicherten individuellen Einstellungen Listen zugelassener Anwendungen für alle im Netzwerk vorhandenen Geräte erstellen.

In eigenständigen Modus wechseln

Um **Dr.Web** in den eigenständigen Modus zu versetzen, entfernen Sie auf dem Einstellungsbildschirm (s. [Abbildung 6](#)) im Bereich **Modus** das Häkchen neben **Dr.Web Agent**.

Beim Aktivieren des eigenständigen Modus werden die Standardeinstellungen oder Einstellungen des Antivirenprogramms, die vor dem Wechsel in den Zentralschutz-Modus vorgenommen wurden, wiederhergestellt. Alle Funktionen von **Dr.Web** können weiterhin verwendet werden.

Um in den eigenständigen Modus zu wechseln, brauchen Sie eine gültige private [Lizenz](#). Die Lizenz, die Ihnen vom Zentralschutz-Server automatisch bereitgestellt wurde, kann in diesem Modus nicht verwendet werden. Eventuell müssen Sie eine private Lizenz [erwerben oder Ihre vorhandene private Lizenz aktualisieren](#).

Kapitel 7. Dr.Web für Android TV

Auf Geräten unter Android TV stehen Ihnen folgende **Dr.Web** Funktionen zur Verfügung:

- [Permanenter Virenschutz](#)
- [Überprüfung auf Anforderung des Benutzers](#)
- [Aktualisierung](#)
- [Statistik](#)
- [Quarantäne](#)
- [Bei Beseitigung der Sicherheitslückenhelfen](#)



Abbildung 20. Dr.Web für Android TV

Einige Besonderheiten von Dr.Web für Android TV

Lizenzierung

- Es ist keine Möglichkeit vorgesehen, eine Lizenz direkt über die App zu [kaufen](#).
- Um Ihre Lizenz zu aktualisieren, müssen Sie zum Abschnitt **Über das Programm** wechseln und auf **Lizenz aktualisieren** tippen.

Oberfläche

- Keine [Widgets](#).
- Keine [Benachrichtigungsleiste](#).
- Da das [Menü](#) nicht verfügbar ist, können Sie die Einstellungen der **Dr.Web** Komponenten nicht ändern.



Anhang

Dieser Abschnitt enthält zusätzliche Informationen über **Dr.Web**:

- [Anhang A. Technischer Support](#)

Anhang A. Technischer Support

Bei Problemen mit der Installation der Produkte nutzen Sie folgende Möglichkeiten, bevor Sie sich an den technischen Support wenden:

- Lesen Sie Produktinformationen und Anleitungen unter <http://download.drweb.com/doc/> durch.
- Lesen Sie häufig gestellte Fragen unter http://support.drweb.com/show_faq/ durch.
- Besuchen Sie **Dr.Web** Foren unter <http://forum.drweb.com/>.
- Stellen Ihre Frage an den Technischen Support oder stöbern Sie in unserem Fundus von Antworten auf häufig gestellte Fragen, der Ihnen im Bereich [Mein Dr.Web](#) zur Verfügung steht.

Wenn Sie es nicht geschafft haben, das Problem zu lösen, dann können Sie eine Frage im Abschnitt http://support.drweb-av.de/support_wizard/ stellen.

Die nächste Vertretung von **Doctor Web** und alle notwendigen Informationen über unser Unternehmen können Sie unter <http://company.drweb-av.de/contacts/offices/> finden.



Schlagwortregister

A

Aktionen bei Bedrohungen 26, 27
Akustische Benachrichtigungen 25
Quarantäne 32
Aktualisierung
Automatische Aktualisierung 31
Einstellungen 31
Antispam 28
Antivirus-Netzwerk 55
Anwendungen
Datenverkehr 47, 48
Eingehende Verbindungen 48
Statistik 47
Verbindungsregeln 48
Anwendungsfiler 57
Arbeitsbeginn 16
Ausgeblendete Geräteadministratoren 51
Autostart-Dateien 22, 23

B

Bedrohungen
Bearbeiten 25, 26
Sperr-Software 27
Systemanwendungen 26
Benachrichtigungen 18
Lizenzablauf 12
Mobiles Internet 44
Benachrichtigungsleiste 18
Benutzerdefinierter Scan 23
Betriebsmodus 55
Blacklist 29

C

Cloud Checker 41
Einstellungen 41
Kategorien von Websites 41
Unterstützte Browser 41

D

Datei an das Virenlabor senden 23, 25, 32
Deinstallation des Programms 13, 14
Demoversion 9
Dr.Web 6
Aktionen 25
Aktualisierung 31

Arbeitsbeginn 16
Benachrichtigungen 18
Betriebsmodus 55
Blacklist 29
Cloud Checker 41
Deinstallation 13, 14
Dr.Web Diebstahlschutz 34, 35, 37, 38, 39, 40
Dr.Web Firewall 42
Einstellungen 21
Einstellungen exportieren 21
Einstellungen importieren 21
Einstellungen zurücksetzen 21
Ereignislog 33
Filtern 28, 29, 31
Filterprofile 30
Funktionen 6, 21
In eigenständigen Modus wechseln 57
In Zentralschutz-Modus wechseln 55
Installation 13
Lizenz 8
Lösen der Sicherheitsprobleme 51
Mein Dr.Web 20
Oberfläche 16
Quarantäne 32
Scanner 23
Schlüsseldatei 8
Spamschutz 28
SpIDer Guard 22
Start 16
Statistik 33
Systemanforderungen 7
URL kürzen 54
Virenschutz 22
Wächter 22
Widgets 18
Dr.Web Diebstahlschutz 34
Anmeldung 35
Deaktivierung 35, 40
Dr.Web Diebstahlschutz Locator 39
Einstellung 35, 37
Einstellungsassistent 35
Freundesliste 38
Passwort 35
Passwort zurücksetzen 40
SMS-Befehle 39
Vertrauenswürdige SIM-Karten 37



Schlagwortregister

Dr.Web Diebstahlschutz Locator 39

Dr.Web Firewall 42

Anwendungsdatenverkehr 46, 47, 48

Eingehende Verbindungen 48

Ereignisse registrieren 50, 51

Internet-Traffic 49

Mobiles Internet einschränken 44

Netzwerkverbindungen 49

Protokoll 50

Dr.Web Icon 22

E

Einstellungen exportieren 21

Einstellungen importieren 21

Einstellungen zurücksetzen 21

Ereignislog 33

F

Fehlalarm 23, 25, 32

Filter 28

Benutzerdefiniert 30

Blacklist 29

Filtermodus 28

Filtern 28

Anrufe 28

Blacklist 29

Gesperrte einsehen 31

Modus 28

Nachrichten 28

Profile 30

Filterprofile 30

G

Gesperrte einsehen 31

Google Play 13, 14

H

Hilfe

Lösen der Sicherheitsprobleme 51

I

Internet-Traffic

Anwendungen 46, 47, 48

Mobil 44

L

Links kürzen 54

Lizenz

Aktualisierung 12

aus Datei laden 10

Erhalt 9

Erwerb 9

Herunterladen 9

Nutzung 10

Seriennummer registrieren 10

Verlängerung 12

Lizenz kaufen 9

Lizenzierung 8

Lösen der Sicherheitsprobleme

Ausgeblendete Geräteadministratoren 51

Priorität bei Behandlung der SMS-Nachrichten 51

Root-Zugriff 51

Sicherheitslücken 51

Software-Konflikte 51

Systemeinstellungen 51

M

Market 13, 14

Mobiles Internet

Benachrichtigungen 44

Nutzungsgrenze 44

N

Netzwerkverbindungen

Aktuelle Aktivität 49

O

Oberfläche 16

P

Permanenter Schutz 22

Persönlicher Bereich Mein Dr.Web 20

Priorität bei Behandlung der SMS-Nachrichten 51

Programm installieren 13

Programm starten 16

Programmeinstellungen

Aktualisierung 31

Dr.Web Diebstahlschutz 35, 37

Einstellungen zurücksetzen 21

Export 21



Schlagwortregister

Programmeinstellungen

- Import 21
- Scanner 23
- URL-Filter 41
- Wächter 22

Programmfunktionen 6

Protokoll

- Anwendungen 51
- Dr.Web Firewall 50

Q

Quarantäne

- Aktionen bei Bedrohungen 32
- Größe 32

R

- Ransomware 27
- Root-Zugriff 51

S

Scan

- Benutzerdefiniert 23
- Fehlalarm 23
- Schnell 23
- Vollständig 23

Scanner

- Benutzerdefinierter Scan 23
- Einstellungen 23
- Schneller Scan 23
- Statistik 23
- Vollständiger Scan 23

Schlüsseldatei

- Aktualisierung 12
- aus Datei laden 10
- erhalten 9, 11
- Herunterladen 9
- Nutzung 10

Schneller Scan 23

Schutzstatus 16

Seriennummer registrieren 10

Sicherheitslücken 51

Software-Konflikte 51

Spamschutz 28

Sperr-Software 27

SpIDer Guard

- Aktivierung 22

Einstellungen 22

Statistik 22

Statistik 33

des Anwendungsdatenverkehrs 47

Scanner 23

Wächter 22

Symbole 6

Systemanforderungen 7

Systemeinstellungen 51

T

Technischer Support 59

U

Unterstützte Browser 41

URL-Filter 41

V

Verbindungsregeln 48

Vertrauenswürdige SIM-Karten 37

Virendatenbanken

- Aktualisierung 31

Virenschutz 22

Vollständiger Scan 23

W

Wächter

- Aktivierung 22
- Einstellungen 22
- Statistik 22

Widgets 18

Z

Zentralschutz 55

